발 간 등 록 번 호
11-1620000-000180-01

국제심포지엄
개인정보보호감독기구의 역할과 위상

International Symposium on the Role and Position of an Institution Protecting Individual Privacy

30 September 2009

Hosted by National Human Rights Commission of Korea

국가인권위원회
National Human Rights Commission of Korea

인사말

친애하는 내외귀빈 여러분!

방금 소개받은 국가인권위원회 위원장 현병철입니다. 먼저 오늘 먼길을 마다하지 않고 이 자리에 고견을 발표해 주기 위해 오신 그린릎 교수님(호주), 마리조르쥬 님(프랑스)과 국정감사 등으로 바쁘신 와중에도 이 자리를 빛내주시기 위해 함께 해주신 이혜훈의원님과 변재일의원님, 연구와 학생 지도로 바쁘신 와중에도 고견을 발표해주시기 위해 오신 염흥렬 교수님, 이인호 교수님, 이항우 교수님 등 내외귀빈 여러분께 깊은 감사의 말씀을 드립니다.

오늘 이 자리는, 정보화시대를 맞이하여 국가나 민간기구의 개인정보 수집 관리 체계가 하루가 다르게 발전해가고 있는데 따라 그 부작용으로 개인정보 유출을 비롯한 침해 문제도 함께 급증하고 있으므로 어떻게 하면 이런 문제를 해결하고 완화할 수 있을지를 모색하기 위해 마련되었습니다.

아시다시피 선진 각국은 이미 오래전부터 독립적인 개인정보보호기구를 설치하는 등의 방법으로 개인정보보호를 위한 노력을 기울여 왔습니다. 우리나라의 경우 다소 늦은 감은 있습니다만 여기 계신 두 의원님께서 국민의 기본권 보호를 위해 헌신적으로 노력하신 결과 각각 준비하신 개인정보보호법안이 현재 국회에 상정되어 있는 상태입니다.

우리 위원회도 2002년 설립 이후부터 현재까지 개인정보 침해 관련 사건을 약 350여건을 접수받고 조사하여 약 30여건에 대하여 권고 등 조치를

취하거나 개인정보보호 관련 법안에 대한 의견표명 등 국민의 개인정보보호를 위해 꾸준히 노력을 해왔습니다.

우리 위원회가 그간의 개인정보 관련 진정사건을 처리하면서 느꼈던 점은 내부적으로 조사 노하우나 실무적인 역량 강화도 중요하지만, 오히려 그보다 중요한 것은 어느 누구에 의해서도 영향을 받지 않고 독립적으로 공정한 입장에서 조사하고 권고하고 의견을 제출할 수 있도록 하는 제도적인 조건의 확보였습니다.

이를 위해 우리사회보다 앞서 개인정보보호기구를 설립하고 다년간 경험을 축적해온 선진국가들의 경험을 살펴보는 것은 매우 유익한 일이 될 것입니다. 오늘 관련 분야에서 세계적인 전문가로 인정받으신 그린릾 교수님과 마리조르쥬님 두분으로부터 풍부한 말씀을 듣고, 또 염흥렬 교수님, 이인호 교수님, 이항우 교수님 등 국내 전문가분으로부터 깊이 있는 토론이 진행됨으로써 개인정보감독기구의 위상과 역할에 관하여 의미 있는 지식공유의 장이 되길 기대합니다.

아무쪼록 이 행사가 우리나라의 개인정보보호를 위한 제도를 갖추어 나가는데 일조하게 되길 기대하면서 인사말에 가름하고자 합니다.

감사합니다.

2009. 9. 30.

국가인권위원회 위원장 **현 병 철**

National Human Rights Commission of Korea

International Symposium on the Role and the Status of Data Protection Authorities

30 September 2009, 13:00-17:00 hours

NHRCK Conference Room (11th fl.)

The National Human Rights Commission of Korea ("NHRCK") has the pleasure to inform you that the International Symposium on the Role and the Status of Data Protection Authorities, established by Art. 19, Para. 1 and 9 of the NHRCK Act, will take place on September 30, 2009 at the NHRCK Conference Room in Seoul. This symposium is expected to contribute to a better cooperation between human rights institutions with respect to the protection of personal data and to raise public awareness of the need for the independence of data protection authorities.

Time	Program
13:05 - 13:30	**Opening Remarks** Prof. Hyun Byung-Chul, Chairperson of the NHRCK
	WelcomeAddress Ms. Lee Hyae-Hoon (Grand National Party), Mr. Byun Jae-Il (Democratic Party)
13:30 - 14:10	**Presentation 1** Independence and powers of data protection authorities Prof. Greenleaf, University of New South Wales
14:10 - 14:50	**Presentation 2** History, structure, and Function of European Independent Data Protection Supervisory Authorities Ms. Marie Georges, Informatics and Liberties Consultant
14:50 - 15:10	**Break**
15:10 - 16:10	**Panel Discussion** - Prof. Youm Heung-Ryol (Soonchunhyang University) - Prof. Lee In-Ho (ChoongAng University) - Prof. Lee Hang-Woo (Chungbuk National Universtiy)
16:10 - 16:50	- General Discussion - Q&A
16:50 - 17:00	**Closing**

국제심포지엄: 개인정보보호감독기구의 역할과 위상

○ 일시 : 2009. 9. 30.(수) 13:00 - 17:00

○ 장소 : 국가인권위원회 배움터2(11층)

○ 주최 : 국가인권위원회

시간	내용
13:05-13:30	**[개회사]** **현병철** (국가인권위원회 위원장) **[축 사]** **이혜훈** (한나라당 국회의원) **변재일** (민 주 당 국회의원)
13:30-14:50 (각 40분)	**[제1발표]** Independence and powers of data protection authorities Graham Greenleaf (University of New South Wales)
	[제2발표] History, structure, and Function of European Independent Data protection Supervisory Authorities Marie Georges (Informatics and Liberties Consultant)
14:50-15:10	**휴 식**
15:10-16:10 (각 20분)	**[토 론]** **한국에서의 개인정보보호관련 쟁점 및 개인정보보호기구의 역할과 위상** **염흥렬** (순천향대 정보보호학과 교수) **이인호** (중앙대 법학전문대학원 교수) **이항우** (충북대학교 사회학과 교수)
16:10-16:50	**종합토론 및 질의응답**

목 차

▣ 발표문

▣ 토론문

발표 1

정보보호기관의 독립과 권한 : 국제기준과 아시아태평양 지역 사례

Graham Greenleaf (University of New South Wales)

1
발 표

Independence and powers of data protection authorities: International standards and Asia-Pacific examples

Graham Greenleaf (University of New South Wales)*

* This paper draws on joint work with both Lee Bygrave and Nigel Waters on Australia, and with Paul Roth on New Zealand. It has been written while I am anInternational Scholar at the Faculty of Law, Kyung-Hee University, Seoul, Korea (2009-10).

1. Introduction

This paper considers the operations of data protection (or information privacy) authorities from the perspectives of (i) the significance of their independence and (ii) the desirable functions for them to have. It focuses on the experience of such authorities in Asia and the Pacific, and ignores for most purposes Europe or the Americas, the two other regions with the most significant experience in this field.

There is relatively little written from a comparative perspective on the independence and functions of data protection authorities, with Stewart (2004, 2004a) providing the most detailed analysis. Bennett and Raab (2003: Chapter 5) and Bygrave (2002: Chapter 4) also provide valuable comparative overviews.

An overview of the development of data protection laws in Asia and the Pacific over the last 21 years is in Appendix 1. The data protection principles in those laws are not compared here.

2. Independence – Thirteen factors influencing its meaning

What is meant by an 'independent' DPA? At least the following are often considered necessary:

- Establishment by legislation rather than any executive order or delegated legislation;
- Ability to investigate free of direction or permission from any other political or governmental authority;
- A fixed term of office, so as to avoid being at the whim of executive dismissal (including remuneration also independent of the executive);

- Removal from office only for defined reasons (inability, neglect of duty or serious misconduct), and with procedural safeguards;
- Immunity against personal law suits relating to performance of official duties;

There are other attributes that enhance the independence of DPAs, including:

- Appointment by Parliament rather than by the Executive;
- Resources of the DPA determined independently of the Executive;
- Powers and duties to report directly on issues to either the Parliament and/or the public;
- Co-appointment to a position which continues for some years after a DPA term expires (eg Court or Tribunal membership), thus reducing conflicts of interest;
- Avoiding conflicts of interests by prevention of Commissioners undertaking other positions; or by requiring in multi-member Commissions the disclosure of interests, and by procedures for resolving disputes between Commissioners.

There are also issues concerning the best structure of a DPA, where views differ on which structure makes a DPA most effective, and which it can also be argued can affect the extent to which a DPA can best withstand informal political or commercial attempts to influence its decisions. These include:

- Should a DPA's powers be given to a sole Commissioner or a multi-member 'Commission'?
- Should a DPA be combined with other authorities such as a Freedom of Information Commissioner or an Ombudsman?
- Should a DPA be part of a broader human rights authority?

At least these 12 factors are relevant to an overall assessment of 'independence', to which one should of course add 'the personal character of the Commisisoner'. Independence does

not in itself create an effective DPA: appropriate powers are also needed. A related question about the structure of DPAs, but not one going directly to the question of independence, is whether public sector and private sector DPAs should be separate or combined. These issues will now be considered, first from the perspective of international standards, and then from that of regional experience in Asia and the Pacific.

3. Independence – International standards

One starting point for an assessment of the significance of independence of data protection authorities is the international agreements and international standards concerning data protection.

3.1. OECD Guidelines (1981)

The OECD Guidelines (1981: Part Four. National Implementation) do not include any requirement for implementation authorities or their independence. Member countries should endeavour to 'adopt appropriate domestic legislation' and 'provide for adequate sanctions and remedies'.

3.2. European Union privacy Directive and 'adequacy' (1995)

In the Directive itself Article 28 requires a supervisory authority in Member States, supplemented by the explanation provided by recitals 62 (independence of supervisory authority) and 63 (powers to investigate.

The principle methodological criteria for assessing the 'adequacy' of data protection regimes of countries outside the European Union are set out by the Article 29 Data Protection

Working Party in its document, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (WP 12 5025/98).[1] While these criteria are not in themselves legally binding on the Commission, they are the considered view of Europe's data protection authorities as to what constitutes "adequacy", and are derived from the Working Party's assessment of the most important requirements of Directive 95/46/EC and other international data protection texts. Moreover, the criteria have formed an important point of departure for Commission decisions on the adequacy of third country regimes.

The core criteria include as part *(ii) Procedural / Enforcement Mechanisms*[2]**:**

> "In Europe there is broad agreement that data protection principles should be embodied in law. There is also broad agreement that a system of 'external supervision' in the form of an independent authority is a necessary feature of a data protection compliance system. Elsewhere in the world, however, these features are not always present. To provide a basis for the assessment of the adequacy of the protection provided, it is necessary to identify the underlying objectives of a data protection procedural system, and on this basis to judge the variety of different judicial and non-judicial procedural mechanisms used in third countries."

The Directive is then interpreted by the Article 29 Working Party as requiring 'some sort of institutional mechanism allowing independent investigation of complaints' and 'a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate' in countries which wish to have their laws regarded as 'adequate' by the EU, but their guidelines do not provide any more precise guidance as to what

---

1) See also European Commission, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data* (Luxembourg: Office for Official Publications of the EC, 1998).

2) Extracts from Article 29 Data Protection Working Party, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP 12 5025/98), pp. 5-7 <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf>

constitutes independence.

3.3. Council of Europe Convention 108 (1981) Additional Protocol (2001)

Convention 108 (1981) had no requirement for a data protection authority (and therefore said nothing about independence), but this was added in 2001. The *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows* (Strasbourg,8.XI.2001) provides:

Article 1 - Supervisory authorities

1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.
2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.
   b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.
3. The supervisory authorities shall exercise their functions in complete independence.
4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.
5. In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

The relevance of this protocol requiring that ‘supervisory authorities shall exercise their

functions in complete independence' is that, since 2008, countries outside the EU are now invited to apply to accede to the Convention and the Additional Protocol. Countries in Asia and the Pacific may, in due course, decide that there are advantages in doing so, in order to obtain free flow of personal information between them and Europe.

3.4. APEC Privacy Framework (absence of) standards (2004)

The APEC Privacy Framework does not include any recommendations or requirements for data protection authorities or their independence. However, some requirement for an independent authority is now included in the cross-border privacy rules system that APEC is attempting to develop.

3.5. Accreditation to international DPA meetings

Accreditation requirements[3] established by the Commissioner's themselves include the following:

1. Legal basis
   The data protection authority must be a public body established on an appropriate legal basis.
   Comment: The legal basis upon which an authority is established underpins its independence and ability to perform functions and demonstrates a jurisdiction's commitment to effective protection of personal data. The legal basis should be of the type normally associated with significant public bodies dealing with citizens' rights in that jurisdiction. Typically this will be primary legislation enacted by the legislature, such as a statute, but depending upon local traditions a suitable Executive instrument may be appropriate. The legal basis should be transparent and have sufficient permanence that it cannot be revoked or changed without reference

3) *Accreditation Features Of Data Protection Authorities*, adopted September 25, 2001 during The 23rd International Conference Of Data Protection Commissioners, Paris, 24-26 September, 2001.

to the legislature.

2. Autonomy and independence
   The data protection authority must be guaranteed an appropriate degree of autonomy and independence to perform its functions.
   Comment: Autonomy requires that an authority be empowered, both in a legal and practical fashion, to initiate and undertake appropriate action without having to seek others' permission. Independence is important for agencies to be able to operate free from political or governmental interference and to withstand the influence of vested interests. Typical guarantees include:
   · *appointment for a fixed term;*
   · *removal only for inability to perform the office, neglect of duty, or serious misconduct;*
   · *the power to report directly to the head of government or legislature and to speak publicly on matters of concern;*
   · *immunity against personal law suit for actions carried out as part of official duties;*
   · *power to initiate investigations.*

These requirements are the considered views of the world's DPAs concerning the essence of their functions and who they consider to be their peers, and set out a strong version of almost all of the factors I listed above as essential, and some of those considered desirable.

These requirements are also consistent with the 'Paris Principles' adopted by the UN in 1993 concerning the status of national institutions for the protection and promotion of human rights (Georges, 2009).

Asia-Pacific Privacy Authorities (APPA) accreditation requirements

APPA only allows as members those authorities that have been accredited to the International Data Protection Commissioners' Conference.

3.6. Draft Data Protection Commissioner's resolution (2009)

The *Draft joint proposal of international standards on the protection of privacy with regard to the processing of personal data* (version 2.3) proposed for adoption at International Data Protection Commissioners' Conference (Madrid, November 2009 requires independence of the monitoring authorities responsible for supervising observance of principles, but does not go into details beyond that.

3.7. Conclusions

An independent supervisory body has become a key element of almost all international data protection agreements and standards since the EU privacy Directive in 1995, though not in the APEC Privacy Framework, nor in the privacy instruments of the 1980s. However, as we will see in the next section, the experience of laws in the Asia-Pacific has been that laws with independent DPAs have been more successful, and that experience has involved DPAs which usually have most of the essential attributes of independence listed above, and commonly have some of the desirable ones as well.

The most desirable structure of such independent DPAs is not indicated by these international standards: whether sole Commissioners or joint Commissions, and whether the data protection function should be combined with other functions, is left open. However, regional experience can provide some valuable lessons concerning these matters.

4. Independence and structure – Regional experience

Have privacy laws been enforced more effectively in Asia-Pacific jurisdictions which have independent data protection authorities? What types of DPAs do they have?

4.1. Jurisdictions with independent DPAs

Australia - Federal Commissioner

The Office of the Privacy Commissioner (OPC) is an independent statutory body established under Part IV of the *Privacy Act 1988*. The Office is funded and serviced by the federal Attorney-General's Department. Appointment of the Commissioner is by the Governor-General (on advice from the Australian Government) for a fixed term of up to 7 years (ss. 19A, 20). Stringent limitations apply to prior termination of an appointment (s. 25), such as "by reason of misbehaviour or physical or mental incapacity" (s. 25(1))). There are a range of other mechanisms in place to ensure the Commissioner's functional independence (e.g., the Commissioner is protected from civil actions (s. 67) and from being sued (s. 64)).

Referring to Australian Privacy Commissioners generally, Waters and Dresner (2000) comment:

> "In all cases, the Commissioner's resources are provided through a sponsoring government department and they are subject to a range of budgetary and other pressures which have led at times to their effective independence being questioned. But this is no different from the situation in most countries, and Australian jurisdictions have not only a strong tradition of respect for the independence of statutory officers but also a highly developed system of administrative law which would allow any 'suspect' decisions to be challenged".

The Australian federal data protection regime is sufficient to satisfy the requirements of Article 28(1) of the Directive for a supervisory authority which "shall act with complete independence".

For the first few years of its existence the Office of Privacy Commissioner was part of the Human Rights Commission, with shared facilities, but it subsequently became separate, with

clearly defined separate funding.

The Australian government is proposing to merge the office of Privacy Commissioner into a new office, that of the Information Commissioner, which will combine freedom of information and privacy functions. There will be three Commissioners (the Information Commissioner and two Assistant Commissioners). The provisions in the draft legislation (2009) are complex and need more clarity, but seem to have the effect that the new Information Commissioner has three sets of functions in relation to FOI (s10), privacy (s11) and additional reporting on government information handling (s 9); the new FOI Commissioner has the FOI functions (s10) but can also perform privacy functions; and the Privacy Commissioner keeps all existing functions under both Privacy Act and other laws (s11) but can also perform FOI functions. It is assumed they will act collegially, but it is not clear what will happen in the event of disagreements.

The federal Privacy Commissioner has jurisdiction in relation to both the private sector and the federal public sector (plus the public sector of the Australian Capital Territory), but for constitutional reasons does not have jurisdiction in relation to the activities of the State and Territory public sectors (including local government).

Australia - Public sector DPAs in 5 States and Territories

In New South Wales (NSW) (1998), Victoria (2000), the Northern Territory (2002), Tasmania (2004) and Queensland (2009) there are Privacy Commissioners to deal with matters concerning the public sectors in these states and Territories.

In all cases they are appointed by the government, not the Parliament, for a fixed term with possibility of renewal. They have statutory protections against dismissal similar to the federal Commissioner. Their budgets are set by the government.

However, the structure of the office of Privacy Commissioner differs significantly between jurisdictions:

- In New South Wales (NSW) there is a sole Privacy Commissioner with no functions other than data protection, except that the Commissioner also has an Ombudsman role in privacy issues generally, not only information privacy (data protection) issues. However, in the current re-development of freedom of information laws in NSW, consideration is being given to combining the new FOI Commissioner and the Privacy Commissioner in a joint Commission.
- Victoria also has a sole Privacy Commissioner with no functions other than data protection. The Commissioner is appointed by the Government for a (re-appointable) term of up to seven years (s. 50). The Commissioner can be suspended by the Governor-in-Council but can only be removed by resolution of both Houses of Parliament (s. 54).
- In the Northern Territory there is a sole Information Commissioner, with combined FOI and privacy functions.
- In Tasmania the Ombudsman is also given the role of administering privacy legislation, and there is no Privacy Commissioner.
- In Queensland, a joint Commission model has been adopted in the *Information Privacy Act 2009* in order to combine the FOI and privacy functions, but with some differences from the proposed federal model. A Privacy Commissioner is to be appointed as a deputy to the Information Commissioner, who can delegate powers to him (s139), and can direct him (s142). All powers will reside initially with the Information Commissioner. The Privacy Commissioner, although oddly described as a member of the Information Commissioner's staff (s141), is to be appointed after advertisement and after consultation with a Parliamentary Committee (s145) and can be re-appointed for up to a total of ten years (s146).

In Tasmania and the Northern Territory, two very small jurisdictions, the Commissioners have had only tiny numbers of complaints concerning privacy and seem have done very little to promote that function of their offices, or to take proactive actions to protect privacy. The Queensland Privacy Commissioner has not even yet been appointed. There is therefore no evidence from Australia as yet concerning the successful combination of data protection with other functions (FOI or ombudsman).

The experience of New South Wales shows how a DPA with a sole Commissioner can be very vulnerable, even though it is independent in theory, if it does not have adequate control of its resources. At its creation in 1999, Privacy NSW had the Commissioner and 6 full-time staff, with a budget of $544,004 for 1998-99.[4] At its peak size (2003-04) it had the Commissioner plus 12 full-time staff, a recurrent budget of a little under $1 million pa. The first Commissioner (Mr Puplick) was also the Anti-Discrimination Commissioner, and his salary was paid from that post. However, he had continuing and public disputes with the government and when he committed a questionable use of his positions it was clear the government would not support his continuation and he resigned. From five years from May 2003 to mid-2008 three different Acting Commissioners were then appointed on short-term and part-time contracts (usually between 3 and 6 months) able to be cancelled at the Minister's absolute discretion. Following a failed attempt in Parliament to abolish Privacy NSW and merge it with the Ombudsman's Office, the government reduced the funding available to Privacy NSW for staffing by approximately half, a position which continued until the appointment of the new Commissioner in 2008. That Commissioner is also part-time, with additional responsibly since July 2009 for guiding the establishment of a new FOI Commissioner's office in NSW. It is quite possible that NSW may move to a model of a joint Commission, combining privacy and FOI. Given the nearly complete ineffectiveness and inaction of Privacy NSW since 2004 (including a failure to publish Annual Reports), that may well be a good result. The NSW experience illustrates the vulnerability of a sole

4) See the Privacy NSW Annual Report, 1998-99, pp. 43-45. Not available electronically.

Commissioner model where both re-appointment of a Commissioner and allocation of resources is under government control, not Parliamentary control.

New Zealand

The Privacy Commissioner is an independent Crown entity. The *Privacy Act 1993* (NZ) provides that the Privacy Commissioner "must act independently in performing his or her statutory functions and duties, and exercising his or her statutory powers" (s13(1A)). The *Crown Entities Act 2004* reinforces this independence by providing that '[a] responsible Minister of an independent Crown entity ⋯ may not direct the entity ⋯ to have regard to or to give effect to a government policy unless specifically provided in another Act' (s105).

The Privacy Commissioner is appointed by the Governor-General of New Zealand on the recommendation of the Minister of Justice (s2), for a period of five years unless a lesser period is stated in the appointment (*Crown Entities Act 2004*, s32). The Commissioner can only be removed for proven misbehaviour (*Crown Entities Act 2004* s39). The Commissioner has a function of commenting publicly on privacy issues (*Privacy Act 1993*, s13) which reinforces independence.

Hong Kong

The Ordinance provides for the establishment of the office of the Privacy Commissioner for Personal Data as an independent statutory authority (s5) to monitor and promote compliance with the Ordinance. Appointment is by the Chief Executive of the Hong Kong SAR, for an initial period of five years with eligibility for re-appointment for one term. The Commissioner may only be removed from office by the Chief Executive with the approval by resolution of the Legislative Council on the ground of (i) inability to perform the functions of his office; or (ii) misbehaviour (s5(5)).

The budget of the Commissioner's Office, provided by the Executive, is around HK$40 million per year ($3.875M euros as at 14/4/09), for an establishment of 39 staff (HKPCO Annual Report 2004-05).

Macao

Macao's *Personal Data Protection Act* (2006) is the most recent data protection law in Asia. Macao's Chief Executive ordered the formation of a supervising authority, the Office for Personal Data Protection (OPDP), in March 2007, and designated Ms. Sonia Chan to be the coordinator. The OPDP can exercise all the legal power attributed to the 'supervising authority' by the Act. As is common legal practice in Macao, the nature of the OPDP is as a 'project' until a law governing the organization of the Office is passed. It is intended that this law will establish an independent authority, but this law has not yet been passed, so the extent of independence of the Macao DPA cannot yet be assessed.

4.2. Jurisdictions with privacy laws lacking independent DPAs

Japan

Japan does not have an independent DPA in relation to either its private sector or public sector privacy laws, certainly not in a way sufficient to meet the accreditation standards of the International Conference of Data Protection Commissioners. *The Act on the Protection of Personal Information* ('PPI Act') is the key legislation setting out basic principles and applying to both the public and private sectors. *The Act on the Protection of Personal Information Held by Administrative Organs* ('PPIHAO Act') applies to agencies in the public sector. Both laws require the relevant Ministries to implement the Acts. The PPHIAO requires Ministry consultation with the Information Disclosure and Personal Information Protection Review Board in some situations.

The Quality of Life Policy Council (2007) concluded that 'it is reasonable to maintain the system in which the relevant minister holds sway', but that the creation of an independent authority was 'a medium or long term task in view of compatibility with international practices' (Japan, Quality of Life Policy Council, 2007:31).

As will be outlined in the second half of this paper, it does not seem that enforcement as a result of supervision by Ministries is effective in Japan in either sector.

Taiwan

Taiwan's *Computer Processed Personal Data Protection Act* was enacted in 1995, influenced by the OECD privacy Guidelines. There is no single oversight body, enforcement being left to the Ministries responsible for each industry sector. This lack of any general supervisory agency is criticised as one of the causes of the ineffectiveness of the Act (Tang, 2009). The Executive Yuan (Cabinet) has been proposing measures to strengthen the Act since 2000 (Tang, 2009), but there is still no proposal for a central supervisory agency.

South Korea

[*Not covered in this version of the paper - to be covered in published version*]

5. Lessons concerning the independence and structure of a DPA

5.1. Independent DPA, or part of a government agency

The data protection regimes in Japan and Taiwan seem to be the least successful in the Asia-Pacific region (other than the very small jurisdictions of Tasmania and the Northern Territory), at least in terms of available evidence of enforcement of the legislation. This is

arguably substantially attributable to their lack of an independent data protection authority.

An independent supervisory body has become a key element of almost all international data protection agreements and standards since the EU privacy Directive in 1995, The Japanese Quality of Life Council seems to recognise this in saying that Japan will need to move in that direction.

The active and relatively effective data protection regimes in the region all involve independent DPAs: New Zealand, Hong Kong, Victoria, NSW and Australia (federal). So does Queensland and it is intended so will Macao.

Of the first ten indicia of independence, these first six DPAs share the following:

- A legislative basis;
- Ability to investigate free of direction;
- Appointment of Commissioners for a fixed term (though re-appointment can still be abused, as in NSW);
- Removal of Commissioners only for specified inadequate conduct, and usually only by Parliament;
- Ability to report directly to the public, and to Parliament through an Annual Report at least, and sometimes through special reports;
- Immunity against personal law suits.

These independent DPAs in Asia and the Pacific however lack the following useful attributes of independence:

- Appointment by Parliament rather than the Executive;
- Resources determined independently of the Executive;

- Guaranteed position post-DPA
- Forbidden to hold other concurrent positions.

From this survey, we can argue that the above six indicia of independence are what is expected of a successful data protection authority in Asia and the Pacific.

5.1. Public sector and private sector DPAs – Joint or combined?

These ten factors relevant to independence apply at least as strongly to a DPA investigating the actions of public authorities as they do to a DPA investigating private sector bodies, and probably even more so. Government agencies are more likely to wish to protect their own powers of surveillance of citizens, and to object to DPA attempts to investigate or limit their use of their surveillance capacities, so it is essential that executive powers cannot be used to prevent appropriate investigation. This raises the additional question of whether, if DPAs need to be independent in relation to both public sector and private sector investigations, there is any justification for separate DPAs for each?

As Georges (2009) argues, the similarities in the technologies and activities of both sectors, and the increasing transfer of data between sectors, points to the desirability of coherence in the regulation of both sectors, and this can best be delivered by a DPA competent to regulate both. I would add that, given that the data protection principles applying to both sectors should be largely the same, the desirability of a consistent body of interpretation of these principles emerging also points toward the desirability of one DPA.

So do questions of cost efficiency point to the same conclusion, assuming both sectors are to be effectively regulated. Across Europe, these considerations have led to their being one national DPA combining jurisdiction over both public and private sectors. The same

conclusion has been reached in Asia and the Pacific in New Zealand, Hong Kong, Macao and Australia (federal DPA), and it is also the preferred model in Canada and in South America. Only in Japan, Taiwan and South Korea are the administration of DPA functions splintered between Ministries, and with different models applying to the public and private sectors. Outside the region, only the USA takes such an approach, which it calls 'sectoral' regulation.

Bennett and Raab (2003: 196) concluded that policy debates of the 1970s produced a consensus that both a single law was the best approach to data protection, and a single authority should administer it in both sectors. This still seems the best approach.

5.2. Sole Commissioner or a multi-member 'Commission'?

Unlike Europe, countries in Asia and the Pacific have no experience in multi-member (or 'collegiate') DPAs, though this model is not unfamiliar in broader human rights Commissions. It is possible that a collegiate Commission may find it easier than a sole privacy/data protection Commissioner to resist pressures from politicians, powerful agencies, and major lobby groups, and to oppose cuts in resources.

5.3. Data protection alone, or in combination with other functions?

Canadian provincial jurisdictions pioneered the combination of a Privacy Commissioner with a Freedom of Information Commissioner (Bennett and Raab, 2003: 196), and that combination is now becoming increasingly common in Australia (Northern Territory, new Queensland legislation, being implemented in the federal jurisdiction, and likely in NSW). It is now found in other countries such as the United Kingdom and Hungary. This seems to be the most comfortable combination of data protection with another function.

The merger of a DPA/Privacy Commissioner role with an Ombudsman is an awkward

combination, because a DPA usually includes a significant role in attempting to influence government policy, and legislation, to take data protection considerations properly into account, and may sometimes involve opposition to government policy. The role of an Ombudsman, however, is usually confined to making administration (principally, of legislation) work more fairly and efficiently, and an Ombudsman usually avoids being embroiled in policy and legislation issues, so as to better preserve his ability to negotiate satisfactory outcomes for complainants. The only experience we have so far, of the Tasmanian Ombudsman doing nothing noticeable about his privacy responsibilities, is not encouraging.

5.4. Part of a broader human rights authority?

There is no experience in Asia and the Pacific with a DPA being one member of a broader human rights authority. In jurisdictions which do not have a separate FOI Commissioner, such inclusion of a DPA in a broader structure is one way to give a Privacy Commissioner more protection against pressures from both the public and private sectors.

6. Powers and functions- Which are needed for effective regulation?

How do we best classify the functions and powers of DPAs, and how do we assess their effectiveness in ensuring compliance with data protection principles? First we will consider this from a theoretical perspective, and then consider what minimum standards are suggested by international agreements and standards. Then the experience of data protection regimes in the region will be considered, both from the perspective of what it indicates about standards in practice, and what we know about the effectiveness of the existing regimes.

6.1. Classification – Reactive and proactive powers and functions

DPAs in practice undertake a very wide range of activities, and legislation usually requires or authorises them to do so. How should we classify those activities so as to better understand them? Classification also make the task of assessing the effectiveness of a particular regime easier, because it is then easier to see how one activity might substitute for another that is classified in the same way.

The principal distinction in functions, I suggest, is between those that are reactive and those that are proactive, essentially the same distinction as Bygrave makes between 'reactive and anticipatory forms of control' (2003:85). A DPA can react to external events (either by compulsion or voluntarily), which means that external events determine the DPA's allocation of resources for ensuring compliance. Alternatively a DPA can make strategic choices to determine the priority for use of compliance resources, utilising those powers with which it is provided to carry out such pro-active activities. Finding a good balance between reactive and proactive methods of ensuring compliance is a major task in the design of a data protection regime.

Reactive functions and powers include the following:

- Powers to investigate potential breaches on the basis of complaints received;
- Power to investigate complaints on the request / direction of a Minister / other agency;
- DPA requirement to conduct Privacy Impact Assessments (PIAs) on the basis of an event triggered by legislation, or at the request of a Minister;
- Powers to decide whether to relax or vary Principles on applications by data controllers;
- Powers to develop sectoral codes of conduct only on request of industry bodies or Ministers.

Proactive powers and functions include the following:

- Power to investigate potential breaches on the DPA's own initiative ('own motion');
- DPA powers to seek injunctions / Court orders to enforce principles;
- DPA powers to prosecute for / seek prosecution of breaches;
- DPA powers to audit data controllers; and to decide whether to publish the results;
- DPA powers to decide whether to conduct PIAs; and whether to publish the results;
- Powers to develop sectoral codes of conduct on own initiative.

As Bygrave says [i]n practice, the distinction between reactive and anticipatory controls tends to blur' (2003:85). For example, legislation may set the conditions under which a DPA could conduct an audit or a PIA, but the DPA may have a discretion whether to do so (often based on resource availability).

Bygrave also posits a distinction between 'paternalistic and participatory control forms', and says most data protection regimes exercise a mixture of both (2003: 86).

6.2. Assessment – The standard of 'responsive regulation'

Bennett and Raab (2003: 207) point out that a 'highly efficacious data protection system' does not only require 'an active and assertive regulatory authority', but also requires (in brief) 'a strong and unambiguous law' (both in relation to principles and compliance powers), 'a strong commitment by data controllers' (including to collecting less data), market incentives to the private sector to protect privacy, 'a vigilant, concerned and activist citizenry', and some use of privacy-enhancing technologies (PETs) particularly 'at the outset of system development'. I entirely agree with this summary of what is needed for a complete system, but in this article we are primarily concerned with how the effectiveness of the role of the DPA may be measured, including the compliance powers the DPA has at its disposal.

How should effective enforcement of privacy regulations be measured? I suggest the theory of ‘responsive regulation’, which posits a pyramid or hierarchy of enforcement options, credible use of the whole pyramid of options, and various types of transparency and feedback mechanisms. Ayres and Braithwaite (1992) have summarized some key aspects of their theory of responsive regulation as follows:

> Chapter 2 seeks to solve the policy problem that regulatory styles which are cooperative on the one hand or punitive on the other "may operate at cross-purposes because the strategies fit uneasily with each other as a result of conflicting imperatives." ⋯ it is contended that the achievement of regulatory objectives is more likely when agencies display both a hierarchy of sanctions and a hierarchy of regulatory strategies of varying degrees of interventionism. The regulatory design requirement we describe is for agencies to display two enforcement pyramids with a range of interventions of every-increasing intrusiveness (matched by ever-decreasing frequency of use). Regulators will do best by indicating a willingness to escalate intervention up those pyramids or to deregulate down the pyramids in response to the industry's performance in securing regulatory objectives.
>
> Finally, it is argued that the greater the heights of tough enforcement to which the agency can escalate (at the apex of its enforcement pyramid), the more effective the agency will be at securing compliance and the less likely that it will have to resort to tough enforcement. Regulatory agencies will be able to speak more softly when they are perceived as carrying big sticks.

Theorists such as John Braithwaite and Christine Parker also stress that responsive regulation contains a ‘storytelling orientation’ where stories about the implementation each level of the enforcement pyramid - both successes and failures - are made known to the various classes of stakeholders in the regulatory system (including those who are regulated, the intended beneficiaries of this, and those responsible for assessing its effectiveness). Braithwaite says (in an address to APEC Privacy seminar, Canberra, January 2007) that one test of responsive regulation is how good a system is in ‘bubbling up’ stories of its successes and failures,

provided these stories have credibility as being representative, and that this applies to privacy regulation. Use of each level of sanction must be visible to those regulated, and to consumers or citizens affected by privacy breaches. Publication of details of decisions and other enforcement activities by regulators is therefore essential for responsive regulation to occur.

7. Powers and functions – International standards

What guidance can we obtain from international privacy agreements concerning what are the appropriate enforcement powers to be provided to a DPA? As we shall see, the answer is 'not as much as we might expect'.

7.1. OECD's minimal requirements

The minimum enforcement provisions required by the OECD Guidelines[5] are for legislation which provides reasonable means for individuals to exercise their rights, and adequate sanctions and remedies. Self regulation can also be provided.

7.2. Council of Europe Convention 108 Additional Protocol's higher requirements

Convention 108 (1981) was initially similar but even more cryptic, only required 'appropriate sanctions and remedies for violations of provisions of domestic law giving effect

5) PART FOUR. NATIONAL IMPLEMENTATION
19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:
a) adopt appropriate domestic legislation;
b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
c) provide for reasonable means for individuals to exercise their rights;
d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
e) ensure that there is no unfair discrimination against data subjects.

to the basic principles'[6].

However, the Additional Protocol (2001) to Convention 108 provides considerable more detail:

Article 1 - Supervisory authorities

1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.
2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.
   b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.
3. The supervisory authorities shall exercise their functions in complete independence.
4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.
5. In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

Convention 108 and the Additional Protocol are now open to accession to non-European states that meet their standards.

---

6) Article 10 - *Sanctions and remedies* Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

7.3. European Union Directive requirements and its 'adequacy' standard

In the EU privacy Directive, the key requirements for properly constituted DPAs within the EU are found in Articles 22-24 (judicial remedies and sanctions), Article 27 (codes of conduct), and Article 28 (supervisory authority), supplemented by the explanation provided by recitals 54 (need for a judicial remedy and compensation for damage), 61 (desirability of codes of conduct), 62 (independence of supervisory authority) and 63 (powers to investigate, intervene in legal cases, and help to ensure transparency of processing).

The Directive requires many specific features of EU DPAs (see Bygrave, 2003: Ch 4):

- A right to be consulted when administrative measures or regulations concerning data protection are drawn up (A 28(2));
- Powers to monitor, investigate and intervene in data processing operations (A 28(3);
- Power to hear complaints and take court action concerning breaches of the law (A 28(4));
- Required to maintain a publicly accessible register of processing requiring registration (Arts 18-19);
- DPAs may be empowered to operate a system of 'prior checking' of processing operations 'likely to present specific risks to the rights and freedoms of data subjects' (A 20);
- Ability to exercise their powers in ways which facilitate cooperation with other DPAs (A 28(6)).

Bygrave considers that '[t]he Directive is silent on whether [DPAs] shall be able to impose fines and order compensation for damages though such competence would clearly be compatible with the Directive' (2003: 72). The A 28(3) powers of intervention can be

interpreted either way, he argues.

The Directive also includes provisions about ensuring compliance which are not directly about DPAs:

- Data subjects must be given a 'judicial remedy' for any breaches of their data protection rights, (A 22), but direct access to the courts by data subjects (rather than via complaints to DPAs) to enforce their rights is allowed but not required (Bygrave , 2003: 78);
- There must be a right to appeal against DPA decisions (A 28(3), but it can probably be limited to questions of law and not allow appeals on questions of fact (Bygrave, 2003: 78);
- Rights to obtain compensation are required (A 23(1), subject to exemptions being allowed where data controllers can show they are not responsible for the breach (A 23(2), but it is unclear (though likely) that this covers non-economic (ie emotional) harm as well as economic loss (Bygrave, 2003: 78).

The EU 'adequacy' standard

The Article 29 Working Party's recommended approach to assessing adequacy involves consideration of three aspects of procedural and enforcement mechanisms[7]: (i) delivery of a

7) The Article 29 Working Party states this as: "The objectives of a data protection system are essentially threefold:
   1) to deliver a *good level of compliance* with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.
   2) to provide *support and help to individual data subjects* in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.
   3) to provide *appropriate redress* to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which allows

"good level of compliance" with the content rules (data protection principles); (ii) provision of support and help to individual data subjects in the exercise of their rights; and (iii) provision of appropriate redress to the injured party where rules are not complied with.

That the Working Party is referring to more than an effective complaints system can be seen from its elaboration of the first aspect:

> "A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials."

These general criteria need to be read in the context of the more specific requirements for DPAs within the EU, sketched above, as it is these criteria for a DPA which against which the 'adequacy' of the enforcement regimes of third party countries must indirectly be measured through the Article 29 Working Party's three criteria.

7.4. International Privacy Commissioners accreditation requirements

For the purposes of accreditation of DPAs, the International Privacy Commissioners stay at the level of generality of the OECD, but in comments indicate what are and are not 'an appropriate range of functions'.

> 4. Appropriate functions
> The authority must have an appropriate range of functions with the legal powers necessary to perform those functions.

---

compensation to be paid and sanctions imposed where appropriate."

Comment: A data protection authority will have a range of functions in areas such as compliance, supervision, investigation, redress, guidance and public education. An authority must not merely be advisory but must have supervisory powers with legal or administrative consequence.

7.5. Draft International Privacy Commissioners' standards (2009)

The standards under development by the international Commissioners appear as though they will require 'sufficient powers and adequate resources to deal with the claims filed by the data subjects, and to conduct investigations and interventions where necessary to ensure compliance', plus recourse to the courts to enforce those rights[8].

7.6. APEC Privacy Framework's lack of standards

The Framework's implementation aspects in Part IV Section A ('Guidance for domestic implementation'), provisions I - VI, are non-prescriptive in the extreme. They state that members 'should take all necessary and appropriate steps' to identify and remove or avoid 'unnecessary barriers to information flows' (I), but do not include any similarly strong injunctions to take 'all necessary and appropriate steps' to protect privacy. The bias is clear.

The Framework does not require any particular means of implementation of the Privacy

8) 22. Monitoring
1. In every State there shall be one or more supervisory authorities, in accordance with its domestic law, that will be responsible for supervising the observance of the principles set out in this Document.
2. These supervisory authorities shall provide guarantees of impartiality, independence and technical qualification, and will have sufficient powers and adequate resources to deal with the claims filed by the data subjects, and to conduct investigations and interventions where necessary to ensure compliance with the applicable national legislation on the protection of privacy with regard to the processing of personal data.
3. In any case, without prejudice to judicial review to which should be subject to the work of supervisory authorities in the preceding paragraph, the data subject may have recourse to the courts to enforce their rights under the provisions laid down in the applicable national legislation

Principles, stating instead that the means of implementing the Framework may differ between countries (‘Member Economies’ in APEC-speak), and may be different for different Principles, but with an overall goal of compatibility between countries. (II).

In (II) it is made clear that anything ranging from complete self-regulation unsupported by legislation, through to legislation-based national privacy agencies is acceptable to APEC:

> ‘There are several options for giving effect to the Framework and securing privacy protections for individuals including legislative, administrative, industry self-regulatory or a combination of these methods under which rights can be exercised under the Framework.’
>
> ‘In practice, the Framework is meant to be implemented in a flexible manner that can accommodate various methods of implementation, including through central authorities, multi-agency enforcement bodies, a network of designated industry bodies, or a combination of the above, as Member Economies deem appropriate.’

There is mention of the value of complainants having a choice of remedies ‘commensurate with the extent of the actual or potential harm to individuals resulting from such violations’ (V).

Legislation is mentioned as one means of providing remedies but is not required or even recommended (V). In contrast, even the OECD Guidelines 'Part 4 National Implementation' state that ‘Member countries should in particular endeavour to (a) adopt appropriate domestic legislation’ (OECD 19(a)) and a range of other means including 'reasonable means for individuals to exercise their rights' (19(c)), 'adequate sanctions and remedies' (including against data export breaches) (19(d)), and for 'no unfair discrimination' (19(e)). The OECD support for legislation is tepid, but APEC’s is non-existent.

7.7. Conclusions concerning minimum international requirements

The APEC Privacy Framework does not provide for any discernable minimum standards of ensuring compliance with the data protection principles[9]. Most other international agreements and standards (OECD guidelines (1981), Council of Europe Convention (1981), International Privacy Commissioners' (IPC) accreditation requirements (200?) and draft standards (2009)) only include brief and general statements of requirements, but they do covers matter such as sufficient powers of investigation, adequate remedies, and recourse to the courts. The only detailed statements are found in the EU privacy Directive (1995) and the Council of Europe Convention Optional Protocol (2001). It cannot therefore be said that there is a detailed list of minimum requirements, unless a country regards it as desirable for their data protection system to be regarded as 'adequate' or compliant with European standards, in which case the minimum requirements are much easier to determine.

The following powers and obligations of DPAs are stipulated in the various international agreements and standards:

- Powers of investigation (CoE Protocol; EU Directive; IPC draft standards);
- Power to 'hear' complaints (CoE Protocol; EU Directive; IPC draft standards), by individual and representative groups (EU Directive), at least to the extent of mediation;
- Power to intervene in legal proceedings concerting violations of Principles or bring them to the attention of courts (CoE Protocol; EU Directive);
- Right of appeal to the courts (available to both parties) against DPA decisions (CoE Protocol; EU Directive);
- Effective powers of intervention (EU Directive; IPC draft standards) including powers to (i) intervene before processing (EU Directive); (ii) ban and block processing (EU

9) APEC's 'Pathfinder' projects may be moving toward some types of minimum requirements, but that is still quite obscure: see Greenleaf (2009) and Waters (2008).

Directive); (iii) monitor processing (EU Directive); and (iv) refer matters to political institutions (EU Directive);

- Ability to cooperate with other DPAs (EU Directive; CoE Protocol);
- Requirement to report regularly on their activities (EU Directive);
- Maintenance of a publicly accessible register of data processing activities of which they must be notified (EU Directive);
- Appropriate range of functions with legal powers (IPC accreditation; IPC draft standards).

Additional provisions concerning supervision and remedies (not necessarily functions of DPAs) are found in some of the international agreements and standards:

- Remedies embodied in legislation (OECD);
- Recourse to the Courts to enforce rights (IPC draft standards);
- Encourage self-regulation (OECD);
- Reasonable means to exercise rights (OECD; IPC draft standards);
- Adequate sanctions and remedies (OECD; CoE);
- Ensure there is no unfair discrimination against data subjects (OECD).

The focus of these international agreements and standards tends to be more on the reactive rather than the pro-active side of ensuring compliance, with the EU Directive a partial exception.

8. Powers and functions – Regional experience

The second valuable source of 'standards' for ensuring compliance in data protection is for a country in Asia and the Pacific to look to the experience of its peers, the other data

protection regimes in the region. It is not sufficient to merely look at what powers and responsibilities are provided in those statutes (which gives a measure of *de facto* standards), some assessment of their effectiveness (and therefore their sufficiency) should also be made. Just because the APEC Privacy Framework has nothing useful to say on these matters does not mean that this region is bereft of experience[10].

It is not possible in this article to exhaustively examine every aspect of the compliance regimes in twelve jurisdictions (including the Australian States and Territories), as that would take at least one book, but some of the most distinctive and illustrative aspects of each regime can be used as exemplars of good or inadequate practice.

8.1. Hong Kong – the absence of remedies

Hong Kong's Ordinance provides inadequate remedies for complainants, and inadequate powers of enforcement to the Commissioner.

The Commissioner enforces the requirements of the Ordinance through his power to investigate suspected breaches and serve enforcement notices (ss38 to 50). The power of investigation may be exercised either on complaint from an individual who alleges a breach in relation to his or her personal data, or on the Commissioner's own initiative (s38). The Commissioner has extensive investigative powers including powers to enter onto premises (s42(1)) and to require the furnishing of information and production of documents (s44), which complaints show are sometimes (if rarely) used.

10) For a similar argument in relation to the data protection Principles in the APEC Framework, and how they under-represent the *de facto* standards of the region, see Greenleaf (2009).

Inadequate penalties for breaches

If, after investigating, the Commissioner concludes that a data user has contravened a requirement of the Ordinance and that the contravention is likely to continue or be repeated, he may serve an enforcement notice on the data user directing it to take the steps considered necessary to remedy the contravention (s50).

A breach of one of the Principles is not by itself a criminal offence, but a breach of any other requirement in the Ordinance, such as contravention of an enforcement notice, is an offence (s64 and s62(10)). So the Commissioner can enforce the Principles by the threat of criminal sanction implied in an enforcement notice (s50). Non-compliance with such a notice is an offence (s64(7)). The notice may specify steps needed to remedy the contravention. A major limitation on the effectiveness of enforcement notices is that they may only be served where the contravention is likely to be continued or repeated by the data user (s 50(1)(b)). The notice may direct the data user 'to take such steps as are specified in the notice to remedy the contravention' (s 50(1)(b)).

So, while valuable to protect other data subjects against continuing or future contraventions, such notices provide only a limited remedy to the complainant. Where a breach is not due to any systematic deficiency in the practices of the data user but has nevertheless has already resulted in damage to the complainant's reputation, injury to feelings or financial loss, the only remedy provided by the enforcement notice is protection against a repeat or continuation of the breach and no enforcement notice can be issued at all unless there is a likelihood that this will occur.

As a deterrent to future breaches, prosecutions following failure to observe enforcement notices have also been of little value, as they have occurred so infrequently and the resulting financial and other penalties have been small.

Failed compensation provision

Apart from the right to make a complaint to the Commissioner (who has few remedial powers, and no powers to award compensation), the only remedy available to individuals is through an action in the Courts under s 66 of the Ordinance. Complainants have a statutory right of compensation for damage, including injury to feelings, arising from a contravention of the Ordinance, including a breach of a DPP (s66). The data user has a full defence if it can show it has taken reasonable care to avoid the contravention, or if the contravention was because of inaccurate data received from a third party (s 66(3)), so compensation depends on the data user's culpability not the harm caused to the complainant.

To obtain compensation, individuals are therefore required to start a civil action for compensation in a Hong Kong court, with the attendant risk of litigation costs of both parties being awarded against them if their claim fails (normal Hong Kong practice), and no guarantee of anonymity. The Privacy Commissioner cannot assist them in any such litigation (in contrast to the Hong Kong practice in discrimination cases), and any s48 report by him concerning a breach would not be admissible. The claim must be proven *de novo*. No-one has ever successfully pursued a claim under s66, and there have not even been any serious cases before a Court (there was one misconceived attempt). It is not hard to see why: a venue less hospitable to a privacy claim by anyone other than the very wealthy would be hard to find.

The paucity of s 66 cases is somewhat puzzling even though the venue is discouraging. While washing ones dirty linen in public is not very acceptable in Chinese cultures, Hong Kong is a relatively litigious society by Asian standards and there are frequent defamation actions to uphold one's reputation if a 'false accusation' has been made. It may be that the connection has not been made in the minds of litigants and their lawyers that privacy laws can also be used to vindicate reputation.

The Commissioner does not seem to consider it is part of his role to seek to mediate

settlements of disputes by payment of compensation, and compensation payments are not mentioned in his reports of mediated complaints. The Commissioner has no powers to require the payment of compensatory damages, nor any specific function of mediating between the parties to reach a mutually satisfactory outcome. There is some anecdotal evidence of informal settlements between the parties to complaints, but the Commissioner's office has stated that it does not mediate but merely leaves negotiations to the parties, and is not aware of any voluntary compensation paid (Lam, 2005). There are no reported complaints referring to compensation or damages being paid. It seems therefore that complainants are left to their own resources to pursue compensation under s66.

There is therefore no evidence that anyone has ever received one dollar of compensation in nearly ten years of operation of Hong Kong's data protection law. This is in stark contrast with Korea, where compensation is routine when a breach is established, and it also places Hong Kong at odds with the practices in Australia, New Zealand and Canada, where compensation payments are a feature of orders and settlements (though still the exceptions rather than the norm).

The Privacy Commissioner does not have powers under the Ordinance to intervene in s 66 cases to assist complainants, nor does it give him or the AAB powers to award damages. Equivalent bodies in Australian and New Zealand jurisdictions have such roles. The effectiveness of individual remedies is clearly one of the weakest aspects of the Hong Kong system.

Individuals have no right to go directly to the Courts to seek enforcement of the DPPs by injunctions against existing or proposed practices, but can only complain to the Privacy Commissioner. Such rights to see injunctions do exist elsewhere, such as in s 98 of Australian *Privacy Act 1988*.

Complaints - Rights of appeal and review

A complainant may appeal to the Administrative Appeals Board (AAB), a quasi-judicial statutory body (AAB 2009), against a decision of the Privacy Commissioner not to investigate his or her complaint or not to issue an enforcement notice as a result of an investigation into the complaint (s 39(4)). Similarly, a data user can appeal to the AAB against the Commissioner's decision to issue an enforcement notice (s 47(4)). There is no appeal from the decision of the AAB to a Court, but aggrieved parties can seek judicial review of AAB decisions. Individuals have occasionally been prepared to bring AAB cases, and this does give them their 'day in court' with little risk of costs being awarded against them - but the AAB has no powers to award compensation or other remedies.

The lack of avenues of appeal, the scarcity of judicial review cases, and even the small number of AAB cases means that judicial or quasi-judicial interpretation of the Ordinance is slight. The Commissioner and his staff must act as if their interpretation of the Ordinance is correct, but the unpredictability of judicial decisions on privacy statutes everywhere probably makes this unduly optimistic.. The *Eastweek Case* is evidence of that. The meaning of Hong Kong's privacy legislation will therefore largely remain very uncertain until more judicial cases occur, but its interpretation by the Commissioner's office will continue to constitute the *de facto* law. The Commissioner's office has published its own detailed interpretation of the meaning of the DPPs and other key aspects of the Ordinance (HKPCO 2006), an unusual and valuable practice.

Review of enforcement aspects (2009)

The Constitutional and Mainland Affairs Bureau of the Hong Kong Government has released a Consultation Document on Review of the Personal Data (Privacy) Ordinance (August 2009), calling for submissions by 30 November 2009. Among the issues that the Consultation Document raises for consideration are:

- Whether the Commissioner should be able to provide legal assistance to complainants seeking compensation under s66.
- Whether the Commissioner should be able to award compensation.
- Whether contraventions of a data protection Principle should be an offence.
- Whether repeated contraventions of a Principle should be an offence.
- Whether there should be heavier penalties for repeat offenders.

The issues under consideration give a good indication of the level of dissatisfaction with the enforcement aspects of the Hong Kong Ordinance.

8.2. Macao - a more complete range of remedies

Macao's *Personal Data Protection Act* (2006) is very similar to Portugal's legislation in most respects (though also said to be influenced by Hong Kong's Ordinance). As a result it is closer to the EU privacy Directive of 1995 than any other data protection legislation in Asia.

The Office of Personal Data Protection (OPDP) takes the approach that since an EU-style data protection law is quite new to Chinese society, careful implementation is needed, with an initial emphasis on public education. Although many individuals in Macao are not yet familiar with the law, ODPD consider thats, after nearly two years of operation of the OPDP, most of the public and private sector entities in Macao are aware of the Act and that violation of it might be punished with administrative sanction, or even with criminal charges.

Enforcement measures

A wide range of enforcement measures are provided. Individuals can complain to the OPDP, but can also have general recourse to other legal and administrative remedies. Persons who suffer damage as a result of breaches of the Act are entitled to compensation paid by

the controller, unless he proves he is not responsible for the damage (Article 14). A range of civil (administrative) offences are provided for many types of breaches, and the ODPD is responsible for determining fines in such cases. Criminal offences are specified for use of personal data for purposes incompatible with collection; unauthorised data matching, and in other more serious areas. 'Public warning and censure' and 'publication of the judgment' (concerning violations) are specific 'additional penalties', as are prohibitions of processing and erasure of data. Where there is a violation of fundamental rights of an urgent nature, there can be a direct appeal to Court of Final Appeal.

The enforcement provisions are complex and deserve more elaboration than the above summary. We can say that Macao's law has, at least in theory, one of the most comprehensive 'enforcement pyramids' of the data protection laws in the Asia-Pacific. If we ask 'how is it being used?', the answer is that after only two years it is too early to be sure, but there are some early signs of effectiveness. The OPDP publishes a summaries of its cases in its annual report, in Chinese and Portuguese, and has published a few decisions summaries from 2007 on its website, also in English (OPDP website, 2009). None of the cases reported to date involve compensation payments.

The notification/registration system

The Act has a quasi-registration system (but for some processing only), which makes it unusual in the Asia-Pacific. There must be notification to the OPDP within 8 days of most automated processing of data, or processing of sensitive data, unless an exemption from notification is obtained (Article 21). 'Prior checking' (ie authorisation) is required of processing of sensitive data (in some cases), credit information, data matching, or use for secondary purposes (Article 22). The notification is free. The notficiations and authorisations must be published in a public register and in the OPDP's annual report of many aspects of personal data processing in Macao.

In the areas of surveillance and employment services, the OPDP has already started the notification/registration process (mainly in Article 21, but also in Article 22 and the other Articles on which it depends). After briefing sessions to government departments, banks, public bodies, NGOs, as well as private companies, many of them are now submitting notifications. The OPDP intends to implement the notification/registration in a full scale in the coming years (statement at 29th APPA forum, Hong Kong, 2008). The first stage is implementation in the public sector, then in the private sector. It estimates this may take about two years, after which a specific regulation on notification will be formulated. Processing without proper notification is then likely to result in sanctions.

8.3. Australian federal Commissioner – powers without use, or appeal

The Australian federal Privacy Act 1988 (Cth) appears to be another example of a failure of responsive regulation. In theory the Privacy Commissioner has adequate powers, but for a variety of reasons they are not used at all (and nor can complainants appeal against this). The message this conveys to data controllers is that the Privacy Act can be ignored with a low level of business risk.

Individuals may complain to the Australia's federal Privacy Commissioner about any breach of the privacy principles governing federal agencies (IPPs) or of the private sector (NPPs), or other specific sets of data protection principles concerning tax file numbers, credit reporting etc. On average, 1250 complaints are investigated per year, over two-thirds of which are under the private sector provisions.[11] The Commissioner has wide powers to carry out investigations, but they are rarely if ever used. Complainants are first required to attempt to resolve the complaint with the data controller. Most complaints are handled by a process of

11) OPC, supra n. 32, p. 126. By contrast, complaints relating to breach of IPPs counted for only 17% of total complaints closed during the period 1.7.2003-30.6.2004: see OPC, *The Operation of the Privacy Act Annual Report: 1 July 2003 - 30 June 2004* (OPC, Sydney, 2004), section 5.4.2, p. 55.

investigation and mediation, before the Commissioner considers using the power to make compulsory 'determinations'.

Few systematic details are published of complaint outcomes. Since 2003, the Commissioner has published brief anonymised summaries of significant complaints which have been resolved without a determination, now averaging 15 complaints per year.

The Act allows the Commissioner to conduct "own motion investigations", using the investigative powers of the Act if needed, but these cannot result in enforceable determinations. The Act allows representative complaints to be made by one complainant on behalf of a class of complainants, and these can result in enforceable determinations in favour of all members of the class. In the only published instance of this occurring, a consumer NGO represented the class of complainants, and it is possibly no coincidence that this resulted in the only determination to date against a private sector organisation.

The Commissioner has extensive powers to make "determinations" awarding compensatory damages or requiring apologies or remedial acts, in the event that mediation fails (s52). The determination power has only been used eight times in the 16 years of the Act's operation (and four of those were in the same dispute). Views differ on whether this is an indicator of successful resolution of complaints, but the better view is that the absence of determinations has caused both the public and private sectors to believe that the Act can largely be ignored, as no adverse consequences will follow. Anonymised determinations are published by the Commissioner.

Lack of appeals against Commissioner's decisions

Because of constitutional reasons concerning separation of administrative and judicial powers, determinations by the Commissioner cannot be enforced against data controllers without the matter first being re-heard *ab initio* by a Court (although the findings of the

Commissioner are *prima facie* evidence in such a hearing). The Commissioner can also seek enforcement of a determination. If a determination is unfavourable to the complainant, the complainant has no right of appeal to a Court. The complainant can, however, seek judicial review of the Commissioner's decision, which will generally allow review of any issues of law but not a full reconsideration of the merits of the case. There are no reported cases of complainants having obtained judicial review, only a few misconceived applications dismissed by the Courts.

If a determination is unfavourable to a data controller, the data controller has a *de facto* right of appeal to a Court, because it can simply refuse to comply with the determination, forcing the complainant to seek a Court hearing for enforcement which will then constitute a *de novo* re-hearing. No determination has ever been enforced before a Court.

Both complainant and data controller can appeal to the Administrative Appeals Tribunal to seek review of the amount of any compensation awarded in a Determination. The Commissioner has only once awarded compensatory damages in a disputed determination, and in that case the complainant successfully appealed against the low amount awarded.

The *Privacy Act 1988* allows individuals to seek a court injunction against breaches of the data protection principles, or threatened breaches, but otherwise does not allow individuals to go directly to a court to seek remedies for breaches. The Commissioner can seek injunctions from a court but has never done so. The injunction power has only once been used, in a dispute between two commercial organisations. In practice, complainants go to the Privacy Commissioner, not a court, partly because of the risk of the legal costs of the other side being awarded against them.

Northern Territory - a similar story of non-use

The Information Commissioner has investigative powers similar to the federal Commissioner,

and is required to attempt to mediate a complaint before holding a hearing into it (s111). If mediation does not succeed and a hearing follows (in accordance with procedures in Part 7, Division 2), the Commissioner may make one or more orders (s. 115) similar to those that the federal Commissioner can make (including ordering compensation up to A$60,000). Either party can appeal against a decision of the Commissioner to the Supreme Court, but on a question of law only (s129). The lack of an 'all grounds' right of appeal is a deficiency similar to that in the federal legislation. The Commissioner also has power to conduct privacy audits independent of complaints (s86(1)(e)). There are no examples of the Northern Territory Commissioner's use of powers.

Tasmania - another inadequate model

For completeness in terms of Acts which do not allow access to any independent Court or Tribunal, Tasmania's Act should be mentioned as one lacking any enforceable remedies. The Ombudsman has sufficient investigative powers, but may only give advice and make recommendations upon finding a breach of the Tasmanian Act's privacy principles (PIPPs) (s. 22). These recommendations must be tabled in Parliament within five sitting days of receipt (s. 22(3)). This might place some pressure on agencies to resolve complaints for fear of adverse publicity. The Act does not provide data subjects with a means for obtaining a decision compelling compliance with the PIPPs. There is no avenue for enforcement of the PIPPs through the courts or administrative decisions tribunal. The provision of such a mild "name and shame" provision does not in itself satisfy the requirements for adequacy of the Directive or any other international standard (except perhaps the APEC Framework). The Tasmanian Commissioner's website gives no indication that the Act has ever been used.

8.4. Australian States – remedies from independent Tribunals

Two Australian States, Victoria and New South Wales, provide some evidence of a more

effective enforcement system in relation to public sector privacy, and another (Queensland) has just enacted a similar model.

Victoria

The Victorian Commissioner has a range of functions similar to the Commonwealth and NSW Commissioners (s58). Powers which refer to "personal privacy" mean "privacy of personal information" (s3 definition), but quite a few of the Commissioner's powers, including the power to make public statements, refer to "the privacy of an individual" or "the privacy of any class of individual", which are broad enough to cover non-informational aspects of privacy such as bodily intrusions.

The Privacy Commissioner must attempt to conciliate a complaint if he or she thinks that successful conciliation is reasonably possible (s33). If the parties reach agreement following conciliation, any party has 30 days following agreement to request that the agreement be put in writing, signed by all parties and certified by the Commissioner (s33). The agreement can then be registered with the Victorian Civil and Administrative Appeals Tribunal (VCAT), and on registration it becomes an order of VCAT and its terms can be enforced accordingly (s33(5)). If the Commissioner decides it is not reasonably possible that a complaint will be conciliated successfully, the complainant can require it to be referred to VCAT (s. 32).

The VCAT has powers to make a wide range of orders after it hears a complaint (s. 43), including orders:

- restraining the continuation of conduct which was the subject of the complaint;
- that the respondent take reasonable actions to redress loss or damage (including injury to feelings and humiliation), including requiring an organisation to apologise to the complainant;
- for compensation not exceeding A$100,000 (US$87,000) for loss or damage (including

injury to feelings and humiliation);

- for reimbursement of the complainant reasonable expenses in connection with the complaint; and
- for correction of personal information or attachment of an explanatory statement.

These powers are substantially similar to those found in the Commonwealth *Privacy Act 1988* and the NSW *Privacy and Personal Data Protection Act 1998*, except that the maximum amount of compensation is AUD40,000 (US$35,000) in NSW and is not limited in the Commonwealth.

A hearing by the VCAT, and therefore these remedies, are ultimately available to any complainant, irrespective of whether they initially make a complaint to a code administrator (and then to the Commissioner and then the VCAT); or whether their initial complaint is to the Commissioner because no code applies, and then to the VCAT because conciliation fails; or whether the Commissioner or the Minister refers the complaint directly to the VCAT. This is a strength of the Act: at the end of the day, all complainants have access to the same remedies, and to the same independent, quasi-judicial appeals body. Either party can appeal against decisions by VCAT to the Supreme Court of Victoria. However, complainants cannot take their complaints of breaches of the Principles either directly to VCAT or directly to the Courts.

The VCAT can also make interim orders, on the application of a complainant or the Commissioner, to prevent any party taking actions which would prejudice conciliation or any order the VCAT might subsequently make (s38).

If an organisation failed to comply with a VCAT order under s43 restraining the continuation of conduct which was the subject of a complaint, this would be contempt of the VCAT. Criminal penalties can arise if the Commissioner considers that an organisation has

breached the IPPs (or a code) and the breach "constitutes a serious or flagrant contravention" (not defined further) or is not as serious but is repetitive (defined as "engaged in ... on at least five separate occasions within the previous two years") (s44). The Commissioner can issue a "compliance notice", either on his own initiative or on an application by a complainant (s44(5)), requiring the organisation to take specified steps to ensure future compliance (s44(2)). In such cases, the Commissioner has wide powers of investigation (ss36-38). It is an indictable offence for an organisation not to comply with a compliance notice (s48), and there is a right to seek a review of the Commissioner's decision by the VCAT. Other than this, a breach of the Act does not create any criminal liability (s7(2)).

New South Wales

The *Privacy and Personal Information Protection Act 1998* (PPIPA) established the office of the NSW Privacy Commissioner. The Act contains eleven Information Protection Principles (IPPs), which apply to the NSW public sector, including local government and prescribed bodies which are outsourcing data services, but not to the private sector. State-owned corporations are excluded from the IPPs. There are numerous other exemptions, including by codes of practice made by Ministerial regulation and disallowable by Parliament.

There are two avenues by which a person who considers that a public sector agency has interfered with their privacy, can seek a remedy. They may make a complaint to the Privacy Commissioner under Part 4 Division 3 of the Act. Such complaints may relate to any alleged "violation of, or interference with, the [individual's] privacy" (s. 45(1)). These terms are undefined, are broader than information privacy complaints, and can even include complaints against the private sector. Breaches of the IPPs, a code of practice, or the public register principles in Part 6 are specifically included as matters the Commissioner can investigate (s45(2)). The Commissioner must attempt to resolve the complaint by conciliation (s49), and, on completion of an investigation, can only make reports and recommendations (s50), a "privacy Ombudsman". The Commissioner cannot refer complaints directly to the ADT (in

contrast to the situation in Victoria); they must first request internal review by the agency concerned. If a person chooses to make a complaint to the Privacy Commissioner under Part 4, and the Commissioner investigates, this does not prevent the person from also seeking a remedy under Part 5.

The second avenue is that the individual may complain under Part 5 to the agency concerned about a breach of the IPPs, a code of practice, or the public register principles in Part 6 (s. 52), and the agency must then conduct an internal review (s. 53). The agency must then notify the Privacy Commissioner, and it may request the Commissioner to undertake the internal review on the agency's behalf (for a fee) (s54). If the person is dissatisfied by the internal review, or the action taken by the agency as a result, he or she may apply to the NSW Administrative Decisions Tribunal (ADT) for a review of the conduct that was the subject of the review (s. 55(1)). Within the Tribunal there is a right of appeal from a decision of a single member of the Tribunal to the Appeal Panel of the Tribunal. Further appeal to the NSW Court of Appeal is then possible.

The Tribunal may decide to make any one or more of the following orders (s. 55(2)):

"(a) subject to subsections (4) and (4A), an order requiring the public sector agency to pay to the applicant damages not exceeding $40,000 by way of compensation for any loss or damage suffered because of the conduct;
(b) an order requiring the public sector agency to restrain from any conduct or action in contravention of an information protection principle or a privacy code of practice;
(c) an order requiring the performance of an information protection principle or a privacy code of practice;
(d) an order requiring personal information that has been disclosed to be corrected by the public sector agency;
(e) an order requiring the public sector agency to take specified steps to remedy any loss or damage suffered by the applicant;

(f) an order requiring the public sector agency not to disclose personal information contained in a public register;
(g) such ancillary orders as the Tribunal thinks appropriate."

The Tribunal may only make an order for financial compensation if it is satisfied that "the applicant has suffered financial loss, or psychological or physical harm, because of the conduct of the public sector agency" (s. 55(4)).

The Privacy Commissioner must be notified by the Tribunal of any applications for review that it receives (s. 55(6)), and has a right to appear in such proceedings (s. 55(7)).

There have been approximately 150 cases heard by the NSW ADT concerning the NSW privacy legislation, but many have been on very technical issues, and relatively few on issues of substance concerning interpretation of the Principles or the provision of remedies[12]. Only two cases have gone on appeal to the NSW Supreme Court.

Seven ADT decisions have discussed questions of compensation under s55. The Tribunal has generally taken a conservative approach. Damages do not automatically result from proof of loss being caused by the defendant's breach of the Act (eg *NW v New South Wales Fire Brigades (No 2)* ([2006] NSWADT 61). Compensatory awards have been made of A$5,000 for depression and anxiety (*WT v Auburn Council* ([2007] NSWADT 253) and A$7,500 for disclosure of wrongful disclosure of a report containing a misdiagnosis of the complainants' mental state (*JD v NSW Medical Board* (No.2) [2006] NSWADT 345), of A$2,000 for distress caused by an agency sending the complainant's information to the wrong address (*RD v Department of Education and Training* [2005] NSWADT 195).

The enforcement structure of the NSW Act has therefore resulted in a reasonably

12) See Australian Privacy Case Summaries at <http://www.austlii.edu.au/au/other/AUPrivCS/> for summaries of all such cases.

substantial amount of interpretation of the Act, so that the meaning of its provisions are increasingly clarified by the Tribunal. The ADT cases also include reported instances of modest amounts of compensation being paid to complainants. The extent to which these cases encourage other agencies to settle complaints brought to them for internal review by payment of compensation is not known.

Queensland

Queensland's new Act enables persons to make a complaint about the handling of their personal information by an agency first to the agency for internal review (s166(2)), and then if the agency is unable to satisfy the complaint, to the Commissioner who must take all reasonable steps to mediate the complaint (s171). The terms of agreement of successful mediations can be certified by the Commissioner, and the terms then enforced by QCAT (ss172, 173).

The Act is, on paper, too rigid in its timing requirements and gives the Commissioner too much latitude to discontinue complaint investigations because of 'lack of cooperation' by complainants or other reasons (s168). Complainants cannot bypass the Commissioner and go directly to the Tribunal after internal review by an agency (in contrast to NSW), or to the Courts (s39). Much will depend on the Act being sympathetically administered.

If mediation is unsuccessful, then at the request of the complainant (only), unresolved complaints must be referred by the Commissioner to QCAT (s176). Following a hearing, QCAT will be able to make orders for a range of remedies for breaches of the privacy principles (s178), including requiring injunctions against continuing breaches, apologies, compensation of up to A$100,000, and reimbursement of expenses in pursuing the complaint. This approach is most similar to that in the Victorian legislation.

Breaches of the IPPs can also result in the Commissioner issuing compliance notices to an

agency, where a breach is 'serious or flagrant', or has occurred on five separate occasions in two years (s158). Agencies must take all reasonable steps to comply or they can be subject to a civil penalty (s160). They can seek a review by QCAT (s161).

The Commissioner has other broad powers including conducting reviews of any systemic privacy issues, reporting results to Parliament, 'conducting compliance audits' of any entities under the Act, commenting on any privacy issues relating to the public sector, and issuing guidelines on the application of the Act and 'privacy best practices generally' (s137). Much will depend on the size of the Commissioner's budget allocation to carry out these tasks, which is subject to government determination, but his/her priorities and exercise of powers are not otherwise subject to direction (s134).

The Commissioner also has a power of approving waivers or modifications of agencies' obligations to comply with the IPPs (s157). Such exemptions are called 'Public Interest Determinations' in the Federal Act, and as in that Act the Commissioner here must be satisfied that such a waiver or modification is in the public interest. In the Queensland Act there are no provisions for public hearings or submissions before such an approval is made, but it is treated as subordinate legislation (s157(2)) and is thus subject to Parliamentary disallowance.

8.5. New Zealand – an improved version of the Tribunal approach

The enforcement of the *Privacy Act 1993* (NZ) is driven by complaints received by the Privacy Commissioner, or the Commissioner's 'own motion' investigations. The Commissioner has substantial investigative powers in relation to both. The Commissioner currently deals with about 650 complaints per year, and most are closed within the year of receipt. Many complaints result in agreed settlements, and the Commissioner will discontinue involvement

once it considers a reasonable settlement offer has been made. The Commissioner does not have any power to make binding orders (except in relation to access charges in the private sector), but may refer appropriate matters (for example where the parties are unable to reach a settlement) to the Director of Human Rights Proceedings to decide whether his office should provide representation (ie legal aid) for the complainant in civil proceedings before the Human Rights Review Tribunal (HRRT). If the Director decides not to provide legal representation, the complainant has the right to take their own case to the Tribunal at their own expense. Since 2005, the Commissioner has referred up to twenty such matters each year to the Tribunal. Complainants may also take their case directly to the Tribunal whether or not the Commissioner has investigated. About twenty privacy cases are filed with the HRRT each year.

The Tribunal has powers to issue declarations (the most common remedy), issue restraining orders against continuing breaches (but not prohibitive injunctions), and to order compensatory damage, including for injury to feelings. The highest damages awarded has been NZ$40,000 (US$28,000), followed by NZ$20,000. There are numerous damages awards for wrongly collecting information, poor security safeguards, wrongly denying access, holding inaccurate information on a database, and wrongful disclosure of information (see Roth 1993-2009 for details).

There is a right of appeal to the High Court against decisions by the HRRT, and a further right of appeal on questions of law only to the Court of Appeal (for which either the High Court must grant leave to appeal, or the Court of Appeal special leave to appeal). There have been 23 privacy appeals heard by the High Court, and one by the Court of Appeal. There are 161 decisions on privacy matters by the HRRT, usually giving full statements of legal reasoning, and often lengthy. The Privacy Commissioner has also published 258 case notes giving the Commissioner's opinions on how the IPPs apply in specific situations. Because of these judicial and quasi-judicial decisions, and administrative interpretations by the

Commissioner, New Zealand has by far the largest body of privacy law (hard and soft) in the Asia-Pacific. Its Act is the most fully 'interpreted', and probably the only one that can be said to benefit from a substantial body of considered interpretation.

8.6. South Korea

[*Not covered in this version of the paper - to be covered in published version*]

8.7. Japan – the absence of any responsibility?

In the absence of any national data protection authority in Japan, enforcement of Japan's privacy law is necessarily fragmented. There also seems to be a lack of information about how effectively the Act is being enforced though this decentralised approach.

Private sector

A complaint about the handling of personal information by a business may be filed with one of four bodies under the PPI Act:

(i) *The business entity concerned* A business operator 'shall endeavour' to 'appropriately and promptly process complaints' (A31).

(ii) *An authorized personal information protection organization* (APIPO) There have been 34 organisations so designated by relevant Ministers under A 37 (as at 31 May 2007), discussed below under self-regulation.

(iii) *A local government department* Heads of local government have the same authority as a competent minister in relation to handling complaints (see below concerning 'Administrative orders').

(iv) *The National Consumer Affairs Council of Japan (NCACJ),* including through one of the local Consumer Affairs Centres. The Basic Policy (Japan, 2006) requires the NCACJ to offer advice, provide training and distribute manuals, to assist 'grievance

organs' such as Consumer Affairs Centres.

There are no specific provisions in the PPI Act allowing persons to make complaints to an APIPO, local government department or NCACJ, or to the 'competent minister' (see below concerning 'Administrative orders'), nor to require that complaints are first made to the business concerned.

The NCACJ prepares and distributes a 'Manual on Complaint Processing for Personal Information' and a 'Summary of Personal Information Protection-related Complaints and Responses'. No English language versions are available. Both NCACJ and the Cabinet Office collect complaint examples, and since 2006 have been exchanging them (Japan, Quality of Life Policy Council, 2007:29).

In financial year 2005, 14.028 complaints were lodged with either local governments or the NCACJ (Japan, Quality of Life Policy Council, 2007:2). How many were lodged with authorized personal information protection organizations is not stated.

In financial year 2007, 12, 728 complaints were stated to be lodged with government or NCACJ, 85% being received by local consumer centres. The principal causes of complaint were fraudulent acquisition of personal information, leakage or loss of data and disclosure beyond the purposes of use (Cabinet Office, 2008). Unfortunately, the figures given add up to over 17,000 complaints, so the percentages given are unreliable. The outcomes of the 12,728 complaints were 'guidance and advice' or 'other types of information provision' in 12,094 cases (95%), and 212 (1.7%) successfully mediated, with most of the rest being introductions to other institutions.

It does not seem that any of these complaints feed in to complaints being investigated by a Ministry, so it is not obvious that any mandatory sanctions arise from so many complaints.

The website of the *National Consumer Affairs Council of Japan* gives summaries of 18 complaints from 2004-07[13], but none since then. There is therefore very little 'feedback' to businesses or the public to indicate what is the outcome of breaches of the Act. An essential element of any system of 'responsive regulation' therefore seems to be missing.

Private sector - Administrative orders

Under the PPI Act, the competent minister (see below) 'may have' a business operator 'make a report' on its handling of personal information (A 32), and the minister may then 'advise' the business operator (A 33). It is not clear whether the report must be about a specific complaint, or how an individual brings matters to the attention of a minister.

When a business has violated any of the data protections provisions (Articles 16-27 except A 19, and A 30(2)), the competent Minister may recommend that the business concerned 'cease the violation concerned and take other necessary measures to correct the violation' (A 34(1)). If the business fails follow the recommendation, and minister finds that 'a serious infringement on the rights and interests of individuals is imminent' it may order the business to take the measures recommended (A 34(2)). Urgent orders may be made under some circumstances without the Minister waiting to see whether a recommendation will be followed (A 34(3)). The normal case is therefore a three stage process: a request for a report by the business; a recommendation; and an order.

The 'competent minister' is 'the minister etc concerned with jurisdiction over the business of the business operator' (A 36), except in the case of personal information relating to employment management, responsibility is shared with the Minister of Health Labour and Welfare. The Prime Minister can also designate competent ministers.

13) NCACJ website <http://www.kokusen.go.jp/jirei/j-top_kojinjoho.html>

In financial year 2007, Ministers collected reports from the businesses they supervise in 83 cases, but did not make recommendations or orders in any case. In financial year 2006 they collected reports in 60 cases and made recommendations in four (Cabinet Office, 2008). Ito and Parker (2008) confirm that there have so far only been a limited number of cases in which enforcement proceedings having been brought under the Act:

> One of the significant enforcement proceedings to date was brought against a regional bank in 2005, which resulted from the bank's loss of three CD-ROMs containing personal information about approximately 1.3 million of its customers.[14] It led to a serious rebuke by the regional Finance Bureau, and the issuing of warnings to individual bank officials. The FSA has, by far, been the most active of the government ministries. Of a total of 83 reports ordered from personal information handlers between April 2007 and March 2008, 78 were by the FSA (mostly on data security measures and measures against leakages). However, no recommendations for improvement were issued during this time.

Unless evidence is available that mere requesting of a report always results in spontaneous offers of remedies where appropriate, it does not seem that Ministerial supervision is playing a significant role in any system of responsive regulation here. Ito and Parker (2008) consider that the Act may be somewhat effective *in terrorem*:

> As in the E.U., the real effectiveness of the Act is that it creates for businesses a greater risk of damage to reputation. In fact, the lack of enforcement action may be attributed, in part, to the nature of Japanese society, with its complex system of business etiquette, in which reputation still carries a tremendous amount of importance. Reputation is acknowledged to be particularly important to both individuals and companies (including, to a lesser extent, foreign companies), as is rigid compliance with administrative rules. Japanese businesses would argue that data compliance issues, like other compliance issues, are taken more seriously than in other countries and that even an informal threat of enforcement will usually be sufficient to jolt a

14) "Michinoku ordered to secure data" (The Japan Times, May 23, 2005).

non-compliant business into action. The nature of enforcement proceedings taken against the regional bank in 2005, including the summoning of its President to appear before the local Finance Bureau, and the issue of warnings to individual bank officials, demonstrate at least some willingness on the part of the authorities to frighten companies, through their officers, into compliance with the Act.

There is not, however, much evidence to support the view that companies in Japan have a better record of data compliance than companies in other countries. In fact, the ongoing stream of headlines in the press concerning breaches of the Act is as least anecdotal evidence to support the view that data compliance issues in Japan are just as prevalent as they are in the other major economies.

Criminal penalties

A breach of one of the information privacy principles is not enough in itself to attract criminal penalties under any of the Acts. Under the PPI Act there must also be a breach of a ministerial order. A violation of a ministerial order under A 34 can result in fines up to ¥30,000 (US$3,000) (and up to 6 months in prison if the data controller is an individual) (A 56 and A 57).

Under the public sector legislation there is no general provision for criminal penalties, but where employees or former employees wrongly disclose or collect personal information under certain circumstances, criminal penalties can result (PPIHAO Act, A 53 - A 55), even when the offence is committed outside Japan (A 56). The Act does not prescribe offences by recipients of such information.

Private dispute resolution bodies

The role of ‘authorized personal information protection organizations’ (APIPO) is set out in part 4 Section 2 (Promotion of the Protection of Personal Information by Private Institutions). The Basic Policy says that it expects they will play ‘an extremely important role’ in Japanese

data protection, particularly to assist businesses to voluntarily resolve complaints.

The competent ministry in a sector may authorise as an APIPO a business that involves itself in the handling of complaints about the personal information practices of other businesses (called 'targets') (A 37). There are some very vague standards with which the applicant must comply (A 39). Each other business 'target' must become a member of the dispute resolution body, and this must be made public (A 41). APIPOs can receive complaints directly from individuals, and target entities are required to cooperate in investigations, and not reject the APIPO's requests 'without justifiable reason' (A 42). Each APIPO is supposed to publish its own guidelines (A 43). The Minister can require reports from an APIPO (A 46) or order it to improve its procedures (A 47), or even revoke its authorisation (A 48). There was one case of a minister requiring a report in 2007 (Cabinet Office, 2008: 4).

The APIPOs have no independent powers. They are not arbitrators in disputes or even specifically empowered to be mediators. They are presumably supposed to be neutral as between their members and complainants, but even this is not clear.

Although there have been 34 organisations designated as APIPOs by relevant Ministers under A 37 (as at 31 May 2007), the number of complaints lodged with them in 2005 is not disclosed by the Quality of Life Policy Council. Although the Council adheres to the Basic Policy line that these private dispute resolution bodies are important, it seems to make some elliptical criticisms of at least some of them. It states that 'less active authorized personal information protection organizations are expected to proactively process complaints and provide information to target entities in the future', and furthermore

> From now on, it will be important to fully publicize the roles of authorized personal information protection organizations to the public and entities and to make efforts to

help improve confidence in these organizations. In addition, it will be necessary for these organizations to proactively engage in personal information leakage cases in order to further enhance their functions.

No evidence of their effectiveness is presented by the Council. In the absence of such information, there is no reason to conclude that the APIPO system is effective.

Public sector

The provision of remedies in Japan's public sector is even more difficult to ascertain. Where decisions by administrative organs concerning access to a person's own record, correction, or suspension of use, are appealed against, the head of the administrative organ who is expected to decide the appeal must consult the Information Disclosure and Personal Information Protection Review Board (PPIHAO Act, A42). The result of such consultation must be made know to all relevant parties including third parties who have objected to the disclosure of a personal information file under an access request.

8.8. Taiwan – Another example of ineffective decentralised enforcement

Under Taiwan's *Computer Processed Personal Data Protection Act* (1995) there is no single oversight body, enforcement being left to the Ministries responsible for each industry sector. Evidence of the enforcement or effectiveness of the Act is lacking, but commentators are of the opinion that the Act is ineffective (Peng, 2003 finds it 'insufficient and flawed'; Tang, 2009 points to 'many defects'; Chuang, 2003 says it is 'full of loopholes'), including because of vague provisions (Peng, 2003; Tang 2009), limited scope (Tang, 2009), and lack of any general supervisory agency (Tang, 2009). There is no known enforcement of the very limited existing provisions for data transfer restrictions.

Proposed reforms

The Executive Yuan (Cabinet) has been proposing measures to strengthen the Act since 2000 (Tang, 2009). A Bill was introduced in 2005, and the Minister of Justice revived calls for passage 2007. The Cabinet of the new government of President Ma presented a Bill to the Legislative Yuan in January 2009, and it is awaiting negotiation between the parties before being presented for a second reading (Tang, 2009). Legislative pressure increased again after the August 2008 bust of the largest yet identity theft ring in Taiwan. The proposed reforms include, as well as broader scope of the Act, stronger remedies including compensation and administrative penalty limits to be increased and class actions suits for breaches permitted (Tang, 2009). However, there is still no proposal for a central supervisory agency. Taiwan's data protection legislation is therefore of very limited effectiveness as yet, but there are reasonable prospects that it is likely to become considerably stronger.

9. Conclusions – Powers and responsibilities for responsive regulation

Given the lack of evidence of any effective enforcement of the decentralised approaches to implementation of data protection laws in Japan and Taiwan, the experience of those jurisdictions can be largely ignored. There is no transparency in how Ministries enforce data protection laws, which may impede a full understanding of what they do. The experience of the USA's decentralised enforcement may be more relevant, because at least some of the enforcement actions by the Federal Trade Commission are effective, but that is beyond the scope of this paper.

The regional experience of enforcement of data protection laws allow some tentative conclusions to be suggested concerning what has turned out to be relatively more effective.

9.1. Effectiveness of enforcement through complaint investigation

First, most activities of regional DPAs are reactive, stemming from their powers to investigate potential breaches on the basis of complaints received. This accounts for the largest allocation of resources by DPAs.

What factors seem to be correlated with effectiveness, or lack of it? Here are some preliminary views base on my observations of the history of DPAs in the region, and the available information:

- DPA's need to be able to investigate on their own initiative ('own motion') (Australia federal; NZ; HK), and not only in response to complaints;
- Power to investigate potential breaches on the DPA's own initiative ('own motion') will be more effective if such investigations have the same status as complaints, and are able to carry the same enforcement consequences (contrast Australian federal Commissioner);
- Independent tribunals are more likely to make enforceable decisions (NZ HRRT; NSW ADT; less so Victorian VCAT) than when enforcement powers are given to a DPA (Australian federal Commissioner);
- Allowing complainants to obtain a hearing by such a Tribunal is essential, whether directly (NZ), after internal review by an agency (NSW), or after investigation by a DPA (Victoria, Qld), and the lack of this is a major defect (Australian federal Commissioner);
- Providing compensation solely through the normal Courts is ineffective (HK);
- Allowing Tribunals to provide substantial amounts of compensation for breaches is not overused or abused, and usually results in relatively small payments, with large payments (over US$20,000) being very rare;
- Restricting offences to where conduct in breach is likely to be repeated means that there are rarely any sanctions for most breaches of the Act (HK);

- Rights of appeal to the Courts, not only on questions of law, but on 'all grounds' (including the interpretation of the facts in dispute) are essential (NZ, Victoria, NSW), and jurisdictions where they are lacking show little development of their law (Australian federal; HK);
- Legal assistance to complainants with meritorious claims increases effectiveness (NZ);
- Objective and detailed reporting by a DPA of the use of its powers, and of the outcomes to complainants (particularly concerning mediated settlements) and respondents is essential for any effective operation of a data protection regime. Without such reporting (a) no one can have any confidence in the effectiveness of the DPA; and (b) neither complainants nor respondents can obtain the feedback necessary for them to regard the regulatory regime as effective and to modify their actions accordingly (by pursuing complaints, avoiding futile complaints, avoiding breaches, or remedying breaches respectively). The most detailed reports, both on the law and the remedies, come from Tribunals (NZ HRRT, NSW ADT), but DPAs can also provide substantial details in reports (NZ Commissioner; HK Commissioner's s48 reports). Less effective regimes have the least detailed reporting (NSW Commissioner, post-2003; Australian federal Commissioner; Japan).

Although there is no obvious correlation with effective enforcement as yet, the following innovative features of some DPAs also seem desirable:

- Ability to accept 'representative complaints' on behalf of a class of complainants, provided there is one actual complainant (Australian federal; NZ; possibly HK); Has only occurred once in Australia, and not at all in NZ.
- Allowing NGOs to act for a complainant (Australian federal); In NZ the Director of Human Rights Proceedings has the power to bring civil proceedings on behalf of a class of individuals (s82(4)).
- Powers to investigate complaints about prospective actions which would breach a

Principle, and injunctive powers to prevent such breaches (Australian federal).

- DPA powers to seek injunctions from a Court to prevent anticipated or actual breaches of Principles seems desirable, but has not be utilised where it exists (Australian federal);
- Ability to arrange for independent mediation to help achieve a settlement (NZ).

DPA powers to directly prosecute breaches (rather than referring them to Police prosecution) have been sought by the HK Commissioner, but are opposed by the HK government as unnecessary (Consultation Document, 2009: 32).

DPA power to investigate complaints on the request or direction of a Minister or other agency does not seem to have played a significant role in the work of DPAs in the region.

9.2. Other functions and powers

The functions of DPAs that are not related to complaint investigation tend to combine both reactive and proactive elements.

Making codes and varying Principles

Almost all of the data protection legislation in the region has provisions allowing for the development of sectoral 'codes of conduct' or the closely-related approach of allowing the modification of privacy Principles for particular classes of data controllers or individual controllers. These provisions vary a great deal. For the Australian private sector codes of conduct can provide full co-regulation, replacing the operation of the Act except for a right of appeal to the Privacy Commissioner. In Australia's Commonwealth and NSW public sectors the Commissioners only have powers to amend the Principles. In Hong Kong a Code of Conduct merely creates a rebuttable presumption that compliance is required, but this can be rebutted if the data controller shows that it has complied with the Act. These differences affect the whole structure of the regulatory system, not only the powers of DPAs.

The role that DPAs can play in developing codes/variations also differs considerably. In Hong Kong the Commissioner can issue codes drawn up by himself or others, and must consult with data users and others as he sees fit (s12). In the Australian private sector, private sector organisations must apply for a code to be prepared by the Commissioner (s18BA) and must provide opportunities for public comment (s18BB) before the Commissioner makes the code, which is not disallowable by Parliament. Public consultations are similarly required in relation to variations to Principles applying to Australia's federal public sector, but these variations are disallowable. In the NSW public sector the Commissioner or an agency can propose a code (s31), the Commissioner must consult (and is criticised for not doing so sufficiently), and the Minister then makes a code proposed under s31 but cannot vary it. The NZ Commissioner can issue a legally binding code of practice on his own initiative or on the application of any person (s47), and must call for submissions before doing so. A code can be disallowed by Parliament.

Irrespective of their form, very few codes or variations of Principles have been developed in most jurisdictions. Codes have played far less a role in the legislation than expected. There have only been two Codes in Hong Kong, both for special reasons (ID cards and credit reporting), and only two are operational in Australia, in very minor areas (Queensland clubs; Market and social research). There have been only 10 modifications of the Principles applying to Australia's federal public sector in 20 years. In New Zealand there are at present only three codes in force, dealing with health information, telecommunications and credit, and two others which only modify one Principle, in relation to particular unique identifiers.

NSW is unusual in having a higher rate of approved codes and exceptions to Principles. There are 11 codes under Pt 3 of the Act after a decade, with 9 more in the queue, but the process does not appear to be abused, even though codes are not statutory rules, so there is no procedure for Parliamentary disallowance. Extensive use has also been made of s41 Directions, whereby the Commissioner exempts agencies from compliance with Principles on public interest grounds.

The general experience of data protection in Asia and the Pacific is that sectoral codes are not of major importance and there are few of them.

Conducting audits and inspections to assess existing compliance

Audits by DPAs of data controllers to assess their compliance with legislation have not become a feature of the region's data protection practice. Australia's federal Act empowers the Commissioner to audit the compliance of public sector agencies, but the Commissioner has abandoned all auditing because or budgetary limitations. The Australian Law Reform Commission (ALRC 2008: 47-6) recommends that the Privacy Commissioner should be empowered to conduct 'Privacy Performance Assessments' (ie audits) of personal information held by private sector bodies. Other Australian DPAs do not have audit powers. The Hong Kong Commissioner has powers to carry out 'formal inspections' (s36), and can report recommendations from inspections applying to classes of data users (s48(1)), but these powers have never been used. The Commissioner has proposed to promote voluntary internal audits or 'Privacy Compliance Audits' (PCAs) but there is no evidence this has occurred.

It is desirable that DPAs with audit powers have not only the powers to decide whether to publish the results, but also an obligation to do so at least where significant compliance difficulties are found. Without such a publication obligation, audits cannot play a role in responsive regulation.

Conducting Privacy Impact Assessments (PIAs)

DPAs in the region have had little in their roles involving Privacy Impact Assessments (PIAs). There are no specific requirement for them to conduct a PIA on the basis of an event triggered by legislation, or at the request of a Minister. Nor do DPAs in the region have specific powers to decide whether to conduct a PIA of a prospective or actual information system which they consider may pose problems. Powers to hold a 'watching brief' and report

on technological developments, and powers to conduct 'own motion' investigations have not been interpreted by DPAs to empower them to conduct something resembling PIAs.

The Australian Law Reform Commission (ALRC 2008: 47-4) recommends that the Privacy Commissioner should be able to (a) direct an agency to provide to it a PIA 'in relation to a new project or development that [the Commissioner] considers may have a significant impact on the handling of personal information; and (b) report to Minister if it does not. The deficiency of this recommendation is that there is no requirement that the PIA be made public. It only proposes a review in five years of whether this should apply to the private sector.

10. References

[Incomplete: The full list of references will be added to the published version of this paper]

Bennett, C and Raab C (2003) *The Governance of Privacy: Policy Instruments in Global Perspective*, Ashgate, 2003

Bygrave, L (2003) *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer, 2003

Georges, M (2009) ""History, Structure, and Functions of European Independent Data Protection Supervisory Authorities", presented at *Symposium: Analyzing the Role and Position of an Institution Protecting Individual Privacy*, Seoul, Korea, 30 September 2009

Greenleaf, G (2009) 'Five years of the APEC Privacy Framework: Failure or promise?' (2009) *Computer Law & Security Report* 25 CLSR 28-43

Stewart, B (2004) 'A comparative survey of data protection authorities - Part 1: Form and structure' (2004) 11(2) PLPR 46 at <http://www.austlii.edu.au/au/journals/PLPR/2004/30.html>

Stewart, B (2004a) 'A comparative survey of data protection authorities - Part 2: Independence and functions' (2004) 11(3) PLPR 81 at http://www.austlii.edu.au/au/journals/PLPR/2004/39.html

Waters, N (2008) 'The APEC Asia-Pacific Privacy Initiative - a new route to effective data protection or a trojan horse for self-regulation?' [2008] UNSWLRS 59, at <http://law.bepress.com/unswwps/flrps08/art59/>

ll. Appendix: An overview of data protection laws in Asia & the Pacific

Twenty-one years of Asia-Pacific data protection

Graham Greenleaf, Asia-Pacific Editor

Published in *Privacy Laws & Business International Newsletter*, Issue 100, August 2009, pgs 21-24

The twenty-one years since *Privacy Laws & Business* commenced publication coincides almost exactly with the development of data protection in Asia and the Pacific (the Americas are a separate story). It is therefore an appropriate opportunity to take a chronological overview of how information privacy or data protection laws in this part of the world have developed while PL&B was obtaining maturity. Of course this only gives part of the picture, because constitutional rights and general provisions of civil and criminal laws may also protect privacy.

The slow growth of data protection laws

There are seven jurisdictions in the region which have enacted data protection laws. As yet, the European Union has not declared whether any of their laws are 'adequate'.

Australia's *Privacy Act 1988* (Cth) only covered its federal public sector, but was the first law in the region to enact a full set of Information Privacy Principles (IPPs), based on the OECD Guidelines, and establishing an office of Privacy Commissioner. The Act was expanded in 1991 to cover credit reporting, and finally in 2001 to include the private sector, but with notable very large exceptions for employment records, for so-called 'small business operators' (defined broadly enough to exempt about 90% of all Australian businesses), political activities and media activities. The Act has relatively strong enforcement provisions, but an unwillingness to use them by a series of Privacy Commissioners, and the absence of

any provisions for complainants to appeal to the Courts, has resulted in only a handful of 'determinations' by the Commissioner, and one significant Court decision, after twenty-one years. So Australia's federal privacy law is still largely unknown territory, and agencies and companies can treat its more difficult provisions as optional in the absence of any evidence to the contrary. Almost all of Australia's States and Territories now have data protection laws for their public sectors, some with more effective enforcement through administrative Tribunals.

Japan has had an *Act on the Protection of Personal Information Held by Administrative Organs* governing public sector data since 1988, but it was strengthened to cover paper-based files and penalties for disclosures in 2003. *The Act on the Protection of Personal Information* provided the first coverage of the private sector in 2003. There are confusing exemptions for 'small business' based on the number of persons covered by their databases, for the media and others. The OECD-influenced principles in the 2003 Act are unexceptional, but their meaning is to a large extent determined by 24 different sets of Ministry guidelines aimed at different sectors. There is no central enforcement body. The Act has been held not to create a private right of action before the Courts, so complainants are left to the mercy of enforcement and mediation by relevant Ministries. There is no evidence of effective Ministerial supervision. Although consumer centres and government receive over 12,000 complaints per year, only a handful of complaint summaries are published, and evidence of the Act's effectiveness is lacking. The Act provides a formal role for 'authorized personal information protection organizations' (APIPO) to help resolve complaints in some way, but how they do this is obscure. The effect of the self-regulatory PrivacyMark system is equally enigmatic.

New Zealand's *Privacy Act 1993* was the region's first comprehensive law governing both public and private sectors and establishing the office of Privacy Commissioner. Its twelve information privacy principles (IPPs) are substantially based upon on the OECD Guidelines

with some Australian influences. It is probably the most effectively enforced law in the region. Most of the approximately 650 complaints per year received by the Commissioner are closed within the year of receipt, many resulting in agreed settlements. However, around twenty per year are referred to the Human Rights Review Tribunal (HRRT), which has powers to make enforceable orders and often does so. The highest damages awarded has been NZ$40,000, followed by NZ$20,000. There are numerous damages awards for wrongly collecting information, poor security safeguards, wrongly denying access, holding inaccurate information on a database, and wrongful disclosure of information. There are rights of appeal to the High Court, which has heard twenty three such cases, and to the Court of Appeal which has heard one. As a result of around 200 such HRRT and Court decisions, New Zealand has rich body of privacy law, and an Act where complainants and respondents alike can understand the consequences of breaches. It is now proposing to remedy its weakest aspect, lack of a data export restriction.

In 1995 the colonial government of **Hong Kong** enacted the *Personal Data (Privacy) Ordinance* (1995), which covered both the public and private sectors. With the 'handover' to China in 1997 the Hong Kong SAR became the first region of the PRC with a data protection law. Six Data Protection Principles are broadly consistent with the OECD privacy Guidelines, but are stronger in some important respects. The main problem with the Ordinance is that there is no provision for the Privacy Commissioner or the Administrative Appeals Board (to whom his decisions can be appealed) to award any compensation or other remedies to complainants, or to penalise organisations for breaches unless they persist with them. A provision allowing Courts to award compensation is unused, probably due to the expense and publicity involved, so the Ordinance suffers from under-enforcement. As a result, chronic data spills go unpunished, and complainants go uncompensated.

Taiwan's *Computer Processed Personal Data Protection Act* was enacted in 1995, influenced by the OECD privacy Guidelines. It has limited coverage, dealing generally with

the public sector but only eight specified private sector areas. There is no single oversight body, enforcement being left to the Ministries responsible for each industry sector. Evidence of the enforcement or effectiveness of the Act is lacking, but commentators are of the opinion that the Act is ineffective. The Executive Yuan (Cabinet) has been proposing measures to strengthen the Act since 2000 (including broader scope, stronger principles and strong enforcement), but to no effect as yet.

Since the 'June struggle' democratic movement of 1987 **South Korea** has changed from authoritarian and undemocratic regimes to a liberal democracy. By 2005 it had the highest distribution rate of Internet broadband networks in the world. These factors have contributed to a society where South Koreans are very conscious of the potential abuses of government power, and of Internet issues, and demand that governments be concerned about privacy protection. Like Australia and Japan, it first introduced a data protection law covering its public sector with the *Public Agency Data Protection Act* of 1995, but it is an Act enforced by the Ministry responsible for government administration, and an oversight body from within government, which are not generally considered to be active or effective. In the private sector, the legislation is to some extent sub-sectoral, with separate laws governing credit and medical information, but the *Act on Promotion of Information and Communications Network Utilization and Information Protection* of 2001 (often called the 'Data Protection Act') applies most generally to entities that process personal data for profit through telecommunication networks and computers. The 2001 Act was influenced strongly by the OECD Guidelines, but was strengthened beyond that in 2004 in relation to data breaches, data exports and other matters. The Personal Information Dispute Mediation Committee (PIDMC) mediates disputes concerning statutory privacy breaches by private sector bodies and provides financial compensation which is enforceable once the mediation is accepted. The PIDMC committees award compensatory damages in almost all cases where a breach of privacy provisions is found, usually even when they award correction or other remedies. Damages typically range from US$100 to US$10,000. The contrast with Hong Kong and most other jurisdictions is

stark. The Korean Information Security Agency (KISA) receives over 17,000 complaints per year, and acts as the secretariat for the PIDMC. Self-regulation has contributed little in South Korea, perhaps due to this effective enforcement. Since 2004 there have been repeated but unsuccessful attempts to fuse the public and private sector provisions into a comprehensive data protection system with an independent supervisory agency.

The **Macao SAR**'s *Personal Data Protection Act* (2006) is the most recent data protection law in Asia, and potentially one of the strongest. The Act is a very similar to Portugal's legislation in most respects (though also influenced by Hong Kong's Ordinance). As a result it is closer to the EU privacy Directive of 1995 than any other data protection legislation in Asia. Macao's position as a region of the PRC makes this doubly interesting. The Office for Personal Data Protection (OPDP) has administered the Act since 2007, and although it has very extensive powers has yet had little time in which to exercise them.

The ASEAN potential, and China

The next stage of development of data protection legislation is likely to come from a number of ASEAN member states that already have official drafts of legislation (Thailand, Philippines, Malaysia and Indonesia), or perhaps from China. ASEAN member countries have made a commitment to develop privacy legislation by 2015.

Thailand's *Official Information Act 1997* provides basic but incomplete data protection in relation to government agencies. It set up a 32-person Official Information Commission (OIC) and a secretariat which serves it. As well as being a freedom of information Act, it also limits personal data collection and its retention, limits disclosures, requires security, and provides access and correction rights. It is, in effect, an information privacy law in relation to the public sector. There are a number of Bills proposing coverage of the private sector, and a privacy Commissioner, but none have been successful, partly due to the current political turmoil.

The **Philippines** has little legislation as yet, but an EU-influenced Act with reasonably strong enforcement powers and a Commissioner is likely to emerge from the legislature in 2009. At present, the *Electronic Commerce Act* (2000) sets a general principle that businesses should give users choice in relation to privacy, confidentiality and where appropriate, anonymity, but it and a set of government guidelines have had little effect. The Supreme Court adopted in 2008 as a rule of Court, a *Rule on the Writ of Habeas Data* which has potential to protect privacy but has not yet been used.

Current privacy protections in **Malaysia** are not significant, and Malaysian Ministers have been monotonously proposing to introduce comprehensive data protection legislation since 1998. However, a new Bill is known to have been prepared in 2009, but no one expects it will provide strong data protection even if enacted.

Indonesia's *Law on Information and Electronic Transaction* (2008) provides a very broad right to compensation for misuse of personal data by electronic media, but is too new to be of significance yet. A draft Bill has been prepared influenced by the OECD Guidelines and other international instruments but is not yet public.

Singapore is arguably the world's only developed country without privacy legislation. Its Model Data Protection Code (2002) is an industry-based self-regulatory code with no known effect. **Vietnam** is considering an APEC reference in a new law, but no privacy developments are known in the remaining ASEAN countries of **Myanmar, Cambodia, Laos** and **Brunei**.

In **China** an EU-style draft *Personal Information Protection Act* was under consideration until 2007, but no longer seems to be under active consideration. It was drafted in 2005 by Professor Zhou Hanhua, director of the Institute of Law at the Chinese Academy of Social Sciences and a team of experts commissioned by the Chinese government. China has no national civil law specifically protecting personal information, but some local governments are

now enacting partial provisions. The Seventh Amendment to the Criminal Law of the PRC (February 2009) criminalises a wide range of disclosures of personal information and the obtaining of same, and is the first time that personal information has been directly protected by the criminal law in China. Any extension of information privacy rights in China will have a strong influence throughout the region.

To complete the east Asian picture, **Mongolia** has taken a unique route, adopting a Law on Personal Secrecy (1995) and Law on Personal Secrecy (Privacy Law), affecting laws covering various types of personal information and creating a right to sue for breaches, and regulate exceptions. There is training for officials, including taking of an oath.

India, outsourcing and South Asia: The recalcitrant zone

South Asia may be the 'final frontier' for data protection in Asia, but the situation there is capable of rapid change. Regional agreements are unlikely to be a factor, as SAARC has shown little interest in privacy, but commercial pressure from Europe may be.

India has no significant data protections laws in force as yet. The *Information Technology Act 2000* covers little of significance to data protection, and has not been enforced. Amendments to it in 2008 may provide remedies for disclosure of 'sensitive' information, but it depends on the regulations yet to be made. The *Credit Information Companies (Regulation) Act 2005* is a potentially significant comprehensive credit reporting code, but it is still being brought into effect by the Reserve Bank of India. The one effective aspect of data protection in India is the right of access to personal information held by any public body in India, under the *Right to Information Act 2005*, which is actively enforced and has already generated a large body of case law. An unknown factor is whether India's Supreme Court might develop the constitutional protection of privacy in such a way that it forces the government to enact a law to provide data protection, as it did in requiring right to information legislation. There is no evidence of any effective self-regulation.

In the rest of the SAARC region (**Pakistan, Bangladesh, Sri Lanka, Nepal, Maldives, Bhutan**) there is no sign of data protection developments, other that a number of Pakistani Bills some years ago which have lapsed.

Conclusions: Slow but accelerating laws with multiple influences

From this brief snapshot of twenty one years of data protection developments, a number of themes emerge. The influences on data protection principles are principally the OECD Guidelines and the EU Directive, but the APEC Privacy Framework has not yet had any direct influence. The influence of the EU Directive is, if anything, strengthening over time. The enforcement/administration model of a central Privacy Commissioner, common in Europe and found in the first regional law (Australia) has continued to find adherents (New Zealand, Hong Kong, Macao and various Bills in Thailand, the Philippines and Korea), but the model of diffuse enforcement responsibilities is also found in North Asia (Japan, Taiwan, proposed in China) though there is little evidence of its effectiveness. Few jurisdictions have yet developed an enforcement structure that generates a significant quantity of Commissioner's case studies or Tribunal/Court decisions to ensure that the law is interpreted, New Zealand being the notable exception.

Overall, data protection laws continue to spread through Asia and the Pacific, and are accelerating if even half of the current Bills are enacted. Existing laws continue to be strengthened, and data export restrictions within the region are becoming more common (Australia, Macao, Korea, Hong Kong though not in effect, and soon New Zealand). Although the APEC processes have had little apparent influence in terms of direct adoption of principles, they may have stimulated data protection interest and legislation. Influences both external and internal to the region are likely to make data protection laws an accepted feature of legal systems across the region before PL&B has another significant anniversary.

1
발 표

정보보호기관의 독립과 권한 : 국제기준과 아시아태평양 지역 사례

그레이엄 그린리프 (호주 시드니 뉴사우스웨일즈 대학 법학교수)*

* 이 글은 호주와 관련하여 리 바이그레이브(Lee Bygrave), 니젤 워터스(Nigel Waters)와, 뉴질랜드에 관하여 폴 로스(Paul Roth)와 함께 한 공동 연구에 바탕을 두고 있다. 이 글은 필자가 한국의 경희대학교 법학부 국제교수로 재직하고 있는 동안(2009-10) 작성하였다.

1. 도입

이 글에서는 정보보호기관(또는 정보 사생활보호 기관)의 운영을, (i) 독립성의 의미, (ii) 기관이 갖추어야 할 바람직한 기능의 관점에서 살펴본다. 아시아 태평양 지역의 기구들의 경험에 초점을 둔 반면에, 이 분야에서 가장 의미 깊은 경험을 지니고 있는 다른 두 지역인 유럽과 미주 지역은 대부분의 경우에 있어 무시하도록 한다.

정보보호기관의 독립성과 기능에 관하여 비교적 관점에서 작성된 글은 상대적으로 드물지만, 그중 Stewart (2004, 2004a)는 가장 세부적인 분석 내용을 제시하고 있다. Bennett와 Raab (2003: Chapter 5), Bygrave (2002: Chapter 4)도 귀중한 비교적 관점의 개관을 제공하고 있다.

지난 21년간 아시아와 태평양에서 정보보호법의 발달에 관한 개요는 <부록 1>에 첨부되어 있다. 여기서는 이 법에 담겨 있는 정보보호 원칙들의 상호 비교는 하지 않도록 한다.

2. 독립성 – 그 의미에 영향을 주는 12가지 요소

'독립적인' DPA란 무슨 의미인가? 이를 위해 최소한 필요한 요소들은 다음과 같다.

- 시행령이나 위임 입법(delegated legislation) 보다는 입법에 의해 설립된다.
- 기타 정치적, 행정적 기관으로부터 지시나 승인을 받지 않고 조사할 수 있는 능력을 갖춘다.
- 행정 집행부의 의도에 따라 갑자기 해임되지 않도록 임기가 정해져 있다(보수 지급도 행정부로부터 독립되어야 함).
- 명시된 이유(무능력, 근무 태만, 중과실 등)에 한해서만 해임된다.
- 공무 수행과 관련하여 사적 소송에 대한 면책권을 지닌다.

DPA의 독립성을 강화할 수 있는 다른 속성으로는 다음을 들 수 있다.

- 행정부가 아닌 입법부(의회)에 의해 임명된다.
- DPA의 자원은 행정부와 독립적으로 결정된다.
- 사안에 관하여 의회와/나 국민에게 직접 보고할 수 있는 권한과 의무가 있다.
- DPA 임기가 만료된 후에도 몇 년간 지속되는 특정 지위(가령, 법원이나 심판소 위원)에 동시 임명함으로써 이해 상충을 줄인다.
- 감독관(Commissioner)이 다른 직위를 갖지 못하게 하거나, 복수 위원으로 구성된 위원회에서 이해 공개를 의무화하고 위원간 분쟁 해결을 위한 절차를 통해 이해 상충을 방지한다.

최상의 DPA 구조에 관하여서도, 어떠한 구조에서 DPA가 가장 효과적일 수 있는지, 그리고 DPA의 결정에 영향력을 행사하려는 비공식적인 정치적, 또는 상업적 시도로부터 가장 잘 맞설 수 있도록 DPA 구조가 어느 정도로 영향을 미칠 수 있는지에 대해서는 다양한 견해가 존재한다. 이와 관련하여 다음과 같은 질문이 제기된다.

- DPA의 권한은 단독 감독관에게 주어져야 하는가, 아니면 다수 위원의 감독기구에 주어져야 하는가?
- DPA는 정보자유위원회(Freedom of Information Commissioner)나 옴부즈맨 기구와 같은 타 기관들과 통합되어야 하는가?
- DPA는 더 포괄적인 인권 기관의 일부여야 하는가?

최소한 이 12가지 요소가 '독립성'의 전반적 평가에 유용하다. 독립성이 그 자체만으로 효과적인 DPA를 보장하는 것은 아니다. 적절한 권한도 필요하다. 독립성 문제와 직접적인 관련되지는 않지만 DPA의 구조에 관한 질문으로, 공공부문과 민간부문 DPA가 별도로 존재해야 하는지 아니면 통합되어야 하는지에 관한 질문이 있다. 이 글에서는 이러한 문제들을, 먼저 국제기준의 관점에서, 그리고 다음으로 아시아 태평양 지역의 경험에 비추어 살펴보도록 한다.

3. 독립성 - 국제기준

정보보호 기관의 독립성의 의미를 평가하기 위한 출발점으로 정보보호에 관한 국제 협약과 국제기준을 들 수 있다.

3.1. OECD 가이드라인(1981)

OECD 가이드라인(1981: 제4부. 국내 이행)은 이행 기관이나 그러한 기관의 독립성에 관한 어떠한 요건도 포함하고 있지 않다. 회원국은 '적절한 국내 법규를 채택'하고 '적정 수준의 제재와 구제를 부과'하도록 힘써야 한다.

3.2. EU 사생활보호 지침(1995)과 '적정성'

EU 사생활보호 지침(EU privacy Directive)은 제28조에서 회원국의 감독기구 설치를 의무화하고 있으며, 이를 보완하는 해설 부분(recitals) 62항(감독기구의 독립성)과 63항(조사권)에서 보다 상세히 설명하고 있다.

EU 외 국가들의 정보보호 체제의 '적정성(adequacy)'를 평가하기 위한 원칙적인 방법론적 기준은 제29조 정보보호 실무단(Article 29 Data Protection Working Party)이 자체 문서인 '제3국으로의 개인정보 이동: EU 정보보호 지침 제25항과 26항의 적용(Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP 12 5025/98))'에 열거하고 있다.[1] 이 기준은 그 자체가 유럽집행위원회에 대해 법적 구속력을 지니고 있지 않지만, "적정성"의 요건이 무엇인지에 관하여 유럽 정보보호기관들의 견해인 것으로 간주되고 있으며, 지침 95/46/EC와 기타 정보보호 국제문건의 가장 중요한 요건들에 대한 실무단의 평가에서 비롯된 것이다. 더 나아가, 이 기준은 제3국 체제의 적정성에 관한 유럽집행위원회의 결정에 있어 중요한 출발점이 되어 왔다.

---

1) European Commission, Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data (Luxembourg: Office for Official Publications of the EC, 1998) 참조.

핵심 기준의 일부인 '*(ii) 절차상/시행 메커니즘*'[2]은 다음과 같다.

"유럽에서는 정보보호 원칙이 법으로 구현되어야 한다는 데에 일반적인 합의가 이루어져 있다. 또한, 독립 기관의 형태를 띤 '외부 감독' 체제가 정보보호 이행 시스템의 필수적 요소라는 점에도 널리 동의하고 있다. 그러나, 유럽 외의 지역에서는, 이러한 요소들이 항상 존재하는 것은 아니다. 제공되는 보호의 적정성 평가를 위한 기반을 제공하기 위해, 정보보호 절차상 체계의 근본적 목적을 파악하고, 이를 바탕으로, 제3국에서 활용되고 있는 다양한 사법 및 사법외 절차상 메커니즘을 판단하는 것이 필요하다.

정보보호 체제는 기본적으로 다음의 세 가지 목적을 지닌다.

1) 양호한 수준의 법규 이행을 달성한다. (어떠한 체제도 100%의 이행을 보장하지는 못하지만, 이행 정도에 있어서 더 나은 체제가 있기는 하다.) 훌륭한 제도의 일반적인 특징은, 정보 관리자가 자신의 의무를 충분히 인지하고 정보 주체는 자신의 권리와 권리를 행사할 수 있는 수단을 충분히 인식한다는 점에 있다. 기관, 감사관 또는 독립적인 정보보호 담당관에 의한 직접적인 검증 체제도 물론 그러하지만, 효과적이고 단호한 제재 실시도 법규 준수를 강화하는 데 있어 중요한 역할을 할 수 있다.

2) 개별 정보 주체가 자신의 권리를 행사하도록 지원을 제공한다. 해당 개인은 신속하고 효과적으로, 그리고 비용 부담 없이 자신의 권리를 행사할 수 있어야 한다. 이를 위해서는, 진정인의 독립적 조사를 허용하는 어떠한 형태의 제도적 메커니즘이 존재하여야 한다.

3) 법규가 이행되지 않은 경우 피해자에 대해 적절한 보상을 제공한다. 보상이 지급되고 필요하다면 제재가 부과되도록 하는 독립적인 심판 또는 중재 제도가 포함되어야 한다.

따라서, 이 지침은 자국의 법규가 EU에 의해 '적정한' 것으로 간주되기를 희망하는 국

2) Extracts from Article 29 Data Protection Working Party, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP 12 5025/98), pp. 5.7 <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf>

가에 '진정인의 독립적 조사를 허용하는 어떠한 형태의 제도적 메커니즘'과 '보상이 지급되고 필요하다면 제재가 부과되도록 하는 독립적인 심판 또는 중재 제도'를 요구하는 것으로 해석되지만, 독립성의 요건에 관하여는 더 상세하게 안내하고 있지 않다.

3.3. 유럽이사회 협약 제108호(1981)와 추가 의정서(2001)

협약 제108호(1981)는 정보보호 기관 설치 요건을 포함하고 있지 않았지만 (따라서 독립성에 대해서도 언급하지 않았다) 2001년에 이 요건을 추가하였다. '감독기구와 국경간 정보이동과 관련하여 개인정보의 자동처리에 관한 개인 보호 협약의 추가의정서 (Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (Strasbourg,8.XI.2001))'는 다음과 같이 적고 있다.

제1조. 감독기구

1. 각 당사국은 이 협약의 제II장과 III장 및 이 의정서에 명시된 원칙들에 효력을 부여하는 자국법의 조치들이 이행되도록 보장할 책임이 있는 1개 이상의 기관을 정하여야 한다.
2. a. 이를 위해, 위 기관은, 이 의정서 제1조의 1항에 언급된 원칙들에 효력을 부여하는 자국법의 조항이 위반된 경우에 법적 절차에 관여하거나 관할 사법당국에 제소하는 권한과 함께, 특히, 조사 및 개입 권한을 지녀야 한다.
   b. 각 감독기구는 개인이 그 기관의 관할권 내에 있는 개인정보 처리와 관련하여 자신의 권리 및 기본적 자유의 보호에 관하여 제기한 진정을 심리하여야 한다.
3. 감독기구는 자체 기능을 완전히 독립적으로 수행하여야 한다.
4. 감독기구의 결정에 대해 진정이 제기되는 경우에는 법원을 통해 항소할 수 있다.
5. 이 협약 제IV장의 조항에 의거하여, 그리고 제13조 조항을 침해하지 않는 범위 내에서, 감독기구는 자체 업무의 수행에 필요한 정도로, 특히 모든 유용한 정보를 교류함으로써 상호 협력하여야 한다.

이 의정서에 '감독기구는 완전히 독립적으로 자체 기능을 수행'하여야 한다고 명시됨으로써, 2008년 이후로 EU외 국가들에 대한 협약 및 추가의정서에 가입 권유가 이루어지

고 있다. 아시아 태평양 지역의 국가들은 이 지역과 유럽간에 개인정보의 자유로운 이동을 보장하기 위해 그러한 가입이 작국에 이로운지를 적정한 시기에 판단하게 될 것이다.

3.4. APEC 사생활보호 기본틀(2004)의 기준 부재

APEC 사생활보호 기본틀(APEC Privacy Framework)에는 정보보호기관 또는 그러한 기관의 독립성에 관한 어떠한 권고나 요건도 포함되어 있지 않다.

3.5. DPA 국제회의에서의 인정 요건

국가 DPA들이 국제회의를 통해 수립한 국제대회 인정 요건[3]은 다음과 같다.

1. 법적 근거
정보보호기관은 적절한 법적 근거에서 수립된 공공기관이어야 한다.

해설: 한 기관의 수립 기반이 되는 법적 근거는 그 기관의 독립성과 업무 수행 능력의 바탕이 되며, 해당 지역의 효과적인 개인정보보호 노력을 입증한다. 법적 근거는 그 관할 지역에서 시민의 권리를 다루는 중요한 공공기관과 통상적으로 연관된 유형이어야 한다. 일반적으로, 법령과 같이 입법부에서 제정하는 일차적 법률일 수 있겠으나, 현지 전통에 따라서는 적절한 행정적 기제도 가능하다. 법적 근거는 투명하여야 하며 충분한 항구성을 지니고 있어서 입법부에 의하지 않고는 철회되거나 수정될 수 없어야 한다.

2. 자율성과 독립성
정보보호기관은 자체 기능을 수행하기 위해 적절한 정도의 자율성과 독립성이 보장되어야 한다.

해설: 한 기관이 자율성을 갖기 위해서는 그 기관에게, 법적으로나 실질적으로, 타 기관의 승인을 구하지 않고도 적절한 행동을 기획하고 취할 수 있는 권한이 주어져야 한다. 독립성은 한 기관이 정치적 또는 정부의 개입을 받지 않고 운영되며

3) 2001년 9월 24-26일에 파리에서 개최되었던 제23차 정보보호기구 국제회의 개최 기간 중인 2001년 9월 25일에 채택된 '정보보호기구 인정 요소(Accreditation Features Of Data Protection Authorities)'

기득권의 영향력에서 벗어날 수 있기 위해 중요한 요소다. 이를 위해 필요한 요소는 일반적으로 다음과 같다.

- *정해진 임기*
- *업무 수행 능력 부재, 근무 태만 또는 중과실이라는 이유에 한하여 해임*
- *정부 또는 입법부의 수반에게 직접 보고할 수 있고 관심사에 대해 공개적으로 의견을 표명할 수 있는 권한*
- *공식 업무의 일환으로 취해진 행동에 대한 사적 소송 면책권*
- *조사 실시권*

이러한 요건들은 DPA 기능의 본질, DPA로 인정할 수 있는 기관에 관하여 전 세계 DPA들이 합의한 견해이며, 앞서 필자가 필수적 요소로서 열거했던 요소들을 거의 대부분, 그리고 바람직한 요소로 꼽았던 것들의 일부를 포함하고 있다.

또한, 이 요건들은 1993년에 UNdl 인권보호와 증진을 위한 국가기구의 지위와 관련하여 채택한 '파리 원칙'과도 일맥상통한다(Georges, 2009).

아시아-태평양 사생활보호 기구(Asia-Pacific Privacy Authorities (APPA)) 인정 요건

APPA는 국제정보보호기구회의(International Data Protection Commissioners' Conference)의 인가를 받은 기관들만을 회원으로 인정한다.

3.6. 정보보호기구 결의안(2009)

국제정보보호기구회의(2009년 11월, 마드리드 개최)에서 채택되도록 제안된 '개인정보처리와 관련된 사생활 보호에 관한 국제기준 공동안(Draft joint proposal of international standards on the protection of privacy with regard to the processing of personal data (version 2.3))은 원칙의 준수를 감독할 책임이 있는 감독기구의 독립을 요구하고 있지만, 그 이상의 세부적인 내용을 다루고 있지는 않다.

3.7. 결론

독립적인 감독기구라는 요건은, 1995년 EU 사생활보호 지침이후로 거의 모든 정보보호 국제협약과 기준에서 주요 요소로 다루어져 왔지만, APEC 사생활보호 기본틀이나 1980년대의 사생활보호 기제에는 포함되어 있지 않다. 그러나, 다음 부분에서 상세하게 다루게 되겠지만, 아시아태평양 지역의 경험에 비추어 보면, 독립적 DPA를 명시한 정보보호법이 더 성공적이었으며 이러한 경험은 대체로 앞서 열거한 독립성의 필수 요소들을 대부분 지니고 있고 상당부분은 바람직한 요소들도 일부 지니고 있는 DPA와 관련이 있다.

그러한 독립적 DPA의 가장 바람직한 구조는 이러한 국제기준에 명시되어 있지 않다. 즉, 단독 감독관과 다수 위원 감독기구 중 어느 것이 더 바람직한지, 정보보호기능이 타 기능과 통합되어야 하는지는 답하고 있지 않다. 그러나, 지역 경험을 살펴보면 이와 관련하여 몇 가지 값진 교훈을 얻을 수 있다.

4. 독립성과 구조 – 지역적 경험

아시아태평양 지역에서 독립적인 DPA를 갖추고 있는 경우에 사생활보호법이 더 효과적으로 시행되었는가? 그러한 경우에 어떤 유형의 DPA를 갖추고 있는가?

4.1. 독립적 DPA를 갖춘 경우

호주 - 연방 감독관

호주의 사생활보호감독관실(Office of the Privacy Commissioner (OPC))은 1998년 사생활보호법 제IV부에 의해 설립된 독립적 법정기구다. 사생활보호감독관실의 재정과 업무 지원은 연방 법무부(Attorney-General's Department)에서 이루어진다. 감독관은 (호주 정부의 조언을 받아) 연방 총독(Governor-General)이 선임하며, 그 임기는 최장 7년으로 정해져 있다 (ss. 19A, 20). 중도 해임은 “과실이나 신체적 또는 정신적 불능의 이유”에 의해

서만 가능한 정도로 엄격한 제약이 주어진다 (s. 25(1))). 이 밖에도 감독관의 기능적 독립성을 보장하기 위한 다양한 메커니즘이 존재한다 (가령, 감독관은 민사 소송(s. 67)과 고소(s. 64)로부터 면책되는 권한을 지닌다).

호주의 사생활보호감독관 제도와 관련하여, Waters와 Dresner(2000)는 다음과 같이 논평한 바 있다.

> "모든 경우에 이 기구의 자원은 담당 정부부서를 통해 제공되며 이 자원은 여러 예산 및 기타 압력에 노출되어 있어서 때로는 이 기구의 효과적 독립성에 의문이 제기되어 왔다. 그러나, 이러한 상황이 다른 대부분 국가와 다른 것은 아니며, 호주의 경우에는 법정 담당관의 독립성을 존중하는 전통이 강할 뿐만 아니라 매우 고도로 발달된 행정법 체계를 갖추고 있기 때문에 '의심스러운' 결정에 대해서는 어떠한 경우에도 이의 제기가 허용되고 있다."

호주 연방 정보보호 체제는 "완전히 독립적으로 행동하는" 감독기구를 명시한 EU 지침 제28조 (1)항의 요건을 충족하기에 충분하다.

사생활보호감독관실은 처음 몇 년간은 인권위원회에 속하면서 시설을 공유하였다가 이후에 별도 기관으로 독립하였다.

호주 정부는 정보감독관실(Office of Information Commissioner)이라는 기구를 신설하고 사생활보호감독관실을 이에 통합시킴으로써 정보의 자유와 사생활보호 기능을 통합할 것을 제안하고 있다. 그렇게 되면 3명의 감독관(Commissioner)이 존재하게 된다(정보감독관과 두 명의 부감독관(Assistant Commissioner)). 법안(2009)의 내용은 복잡하여 좀 더 명료하게 정리될 필요가 있으나, 법안이 확정되면 새로운 정보감독관실이 정보의 자유(FOI) (s 10), 사생활(s 11), 정부의 정보 취급에 관한 추가 보고와 관련한 세 가지 기능을 수행하게 되고, 신설되는 정보감독관(FOI Commissioner)은 FOI 기능(s 10)을 가지면서 동시에 사생활보호 기능도 수행할 수 있게 되며, 사생활보호감독관은 사생활보호법과 기타 법률에 의한 기존 기능(s 11)을 유지하면서 동시에 FOI 기능을 수행할 수 있게 될 것

으로 보인다. 합의에 의한 업무 추진을 전제로 하고 있지만, 감독관들간에 의견이 불일치하는 경우에 어떻게 할 것인가에 대해서는 명확하지 않다.

연방 사생활보호감독관은 민간부문과 연방 공공부문(호주 연방수도자치구(Australian Capital Territory) 포함) 모두에 대해 관할권을 지니지만, 주와 수도자치구의 업무(지방정부도 포함)에 대해서는 헌법상의 이유로 관할권이 없다.

호주 - 5개 주와 자치구의 공공부문 DPA

뉴사우스웨일즈(New South Wales, 1998), 빅토리아(Victoria, 2000), 노던 테리토리(Northern Territory, 2002), 타스마니아(Tasmania, 2004), 퀸즈랜드(Queensland, 2009)에는 해당 주와 자치구에서의 공공부문에 관한 사안을 다루는 사생활보호감독관을 두고 있다.

사생활보호감독관은 모두 의회가 아니라 정부에 의해 임명되고 있으며, 임기는 정해져 있고 연임이 가능하다. 연방 감독관의 경우와 유사한 해임 보호 규정이 법으로 정해져 있다. 예산은 정부가 정한다.

그러나, 감독관실의 구조는 서로 상당한 차이를 보인다.

- 뉴사우스웨일즈의 단독 감독관은 정보보호 외에 다른 기능이 없으나, 정보 사생활(정보보호) 문제뿐만 아니라 사생활보호 전반에 대해 옴부즈맨 역할을 하고 있다.
- 빅토리아의 경우에도 단독 감독관 체제로서 정보보호 외의 다른 기능은 없다. 감독관은 정부가 선임하며 재임 가능하여 임기는 최장 7년이다(s. 50). 주 관할 총독(Governor-in-Council)에 의한 정직은 가능하나 해임은 상하 양원의 결의에 의해서만 가능하다(s. 54).
- 노던 테리토리는 단독 정보보호감독관을 두고 있으며, FOI와 사생활보호 기능을 겸하고 있다.
- 타스마니아에서는 옴부즈맨이 사생활보호법의 이행을 감독하는 역할도 갖고 있으며, 사생활보호감독관은 없다.

- 퀸즈랜드에는 FOI와 사생활보호 기능을 통합하기 위하여 2009년 정보사생활보호법(Information Privacy Act)에 의해 합동위원회 모형이 채택되었지만, 제시된 연방 모형과는 다소 차이가 있다. 사생활보호감독관은 정보감독관의 부감독관으로 임명되며, 정보감독관이 사생활보호감독관에게 권한을 위임할 수 있으며(s 139) 지시를 내릴 수도 있다(s 142). 사생활보호감독관은, 정보감독관실에 속하는 구성원으로 다소 이상하게 묘사되고 있기는 하지만(s 141), 공모를 거친 후에 의회 위원회와 협의하여 선임하여야 하며(s 145) 재임이 가능하여 최장 임기는 10년이다(s 146).

매우 작은 규모의 관할지역인 타스마니아와 노던 테리토리에서는, 사생활보호와 관련하여 제기되는 진정건의 수가 매우 적어서 감독관이 그 기구의 기능을 활성화하거나 사생활보호를 위한 적극적인 조치를 취하는 노력을 거의 기울이지 않는 것으로 보인다. 퀸즈랜드의 감독관들은 아직까지 선임된 적이 없으며, 따라서 호주에서 정보보호와 기타 기능(FOI나 옴부즈맨)이 성공적으로 통합된 증거 자료는 찾아볼 수 없다.

뉴사우스웨일즈의 사례는 단독 감독관 체제의 DPA가 이론적으로는 독립되어 있지만 자원에 대한 적절한 통제 능력이 없는 경우에 얼마나 취약할 수 있는가를 보여준다. 1999년에 설립되었을 당시의 사생활보호감독관실(Privacy NSW)은 1명의 감독관과 6명의 상시 직원으로 구성되어 있었고, 1998-99년 예산은 544,004달러였다[4]. 활동이 최정점에 이르렀던 2003년 4월에는, 상시 직원은 12명으로 늘어났고 연간 예산은 1백만 달러에 약간 못 미치는 수준이었다. 초대 감독관인 Mr. Puplick은 반차별감독관(Anti-Discrimination Commissioner)도 겸임하고 있었으며 이 직책에 대해 보수를 지급받았다. 그러나, 정부와의 갈등이 계속되었고 자신의 직책을 부당하게 이용하였다는 혐의가 가해지면서 정부가 그를 지지하지 않게 되자 사임하였다. 2003년 5월부터 2008년 중반까지 5년 동안, 세 명의 감독관 대리가 단기 및 임시 계약으로 (주로 3~6개월) 이 직책을 거쳐 갔으며, 이러한 계약은 장관의 절대적인 재량에 의해 해지가 가능하였다. 사생활보호감독관실을 폐지하고 옴부즈맨실(Ombudsman's Office)에 통합하려는 의회의 시도가 실패한 후에, 정부는 사생활보호감독관실 소속 인력에 할당된 재정을 거의 절반으로

4) Privacy NSW Annual Report, 1998-99, pp. 43-45 참조. 온라인 버전은 없음.

줄였으며, 이러한 정책은 2008년 신임 감독관이 임명되기 전까지 계속되었다. 신임 감독관은 뉴사우스웨일즈에 FOI 담당관실 설치를 지휘하는 책임을 맡고 있었으므로 실제적으로는 사생활보호감독관으로서의 역할은 비정규직에 그쳤다. 뉴사우스웨일즈가 사생활보호와 FOI를 통합하는 합동위원회 모형으로 전환할 가능성은 매우 크다. 2004년 이후로 (연례보고서 발간도 하지 못할 정도로) 사생활보호감독관실의 실효성과 활동이 거의 전무하다는 점을 감안하면, 바람직한 방향일 수 있다. 뉴사우스웨일즈의 사례는 감독관의 재임과 자원 할당이 모두 의회가 아닌 정부의 통제하에 있는 경우에 단독 감독관 모형이 갖는 취약점을 잘 보여준다.

뉴질랜드

뉴질랜드의 사생활보호감독관은 독립적인 책임운영기구(Crown entity)다. 1993년 사생활보호법은 사생활보호감독관이 “자신의 법적 기능과 임무를 수행하고 자신의 법정 권한을 행사함에 있어 독립적으로 행동하여야 한다”고 명시하고 있다(s 13(1A)). 2004년 독립기구법(Crown Entities Act)은, ‘독립기구의 책임 장관은...다른 법에서 구체적으로 명시하고 있는 경우가 아니라면 해당 기구에 대해...정부 정책을 고려하거나 정부 정책에 효력을 부여하도록 지시할 수 없다(s 105)’고 명시함으로써 이러한 기구들의 독립성을 강화하고 있다.

사생활보호감독관은 법무부의 권고에 따라(s 2) 뉴질랜드 총독이 선임하며, 선임 당시 더 짧은 임기가 명기되지 않는 한 5년의 임기 동안 재직한다(2004년 독립기구법 s 32). 감독관은 과실이 입증되는 경우에 한하여 해임할 수 있다(동법 s 39). 사생활보호 문제와 관련하여 공개적으로 논평할 수 있는 기능을 지니며(1993년 사생활보호법 s 3), 이러한 기능은 독립성을 강화하는 효과가 있다.

홍콩

법령의 이행을 감독하고 증진하기 위한 독립적 법정기구로서 개인정보 사생활보호감독관실(Office of the Privacy Commissioner for Personal Data)의 설치를 법령으로 정하고 있다.

홍콩 특별행정자치구의 총독이 선임하며, 5년의 임기로 1회에 한하여 재임가능하다.

감독관은 (i) 업무 수행 능력 부재, 또는 (ii) 과실을 이유로 입법부(Legislative Council)의 결의에 의한 승인을 얻는 경우에 한하여 총독이 해임할 수 있다(s 5(5)).

사생활보호감독관실의 예산은 총독이 정하며 39명의 인력 고용에 약 연간 HK$ 4천만(2009년 4월 14일 현재 $3,875,000에 해당)에 이른다(2004-05년 HKPCP 연례보고서).

마카오

마카오의 개인정보보호법(2006)은 아시아에서 가장 최근에 제정된 정보보호법이다. 마카오 총독은 2007년 3월에 감독기구인 개인정보보호실(OPDP)의 설치를 명하였고 Ms. Sonia Chan을 실장(coordinator)으로 임명하였다. OPDP는 이 법에 의해 '감독기구'에 주어진 모든 법적 권한을 행사할 수 있다. 마카오의 법관행에서 일반적으로 그렇듯이, OPDP는 해당 기구의 조직을 관할하는 법이 통과하기 전까지는 '프로젝트'의 성격을 띤다. 이 법에 의해 독립적인 기구 확립은 가능하겠지만, 아직까지 이 법이 통과되지 못한 상황이어서 현재로서는 마카오 DPA의 독립성 정도를 평가할 수 없다.

4.2. 사생활보호법은 있으나 독립적 DPA는 없는 경우

일본

일본에는 민간부문과 공공부문의 사생활보호법과 관련하여, 정보보호기구 국제회의의 인정 기준을 충족할 만한 독립적인 DPA를 두고 있지 않다. 개인정보보호법(Act on the Protection of Personal Information ('PPI법'))은 기본 원칙을 수립하고 공공 및 민간부문 모두에 적용되는 핵심 법률이다. 행정기관이 보유한 개인정보보호법(Act on the Protection of Personal Information Held by Administrative Organs ('PPIHAO 법'))은 공공부문의 기관들에게 적용된다. 두 법 모두 관련 부처의 법 이행을 의무로 하고 있다. PPIHAO 법에 의하면 해당 부처는 일부 경우에서는 '정보공개 및 개인정보보호 심의위원회'와 협의하여야 한다.

‘삶의질 정책 위원회’(2007)는, ‘관련 장관이 관할권을 지니고 있는 이 체제를 유지하는 것이 합당하다’고 결론지으면서도 독립적 기관의 신설은 ‘국제관행에 부합한다는 관점에서 볼 때 중장기적 과제’라고 덧붙였다(일본 삶의질 정책 위원회, 2007:31).

이 글의 후반부에서 개략적으로 설명하겠지만, 정부 부서의 감독에 의한 이행은 일본의 민간부문과 공공부문 어디에서도 효과적이지 못한 것으로 보인다.

대만

대만의 ‘전산처리 개인정보보호법(Computer Processed Personal Data Protection Act)’은 OECD 사생활보호 가이드라인의 영향으로 1995년에 제정되었다. 감독기구는 전혀 없으며, 이 법의 시행은 각 산업 부문의 책임 정부부서에 맡겨져 있다. 이 법의 시행 또는 실효성을 보여주는 증거 자료는 부족하지만, 논평가들은 이 법이 실효성이 없다는 데에 의견을 같이하고 있는데(Peng(2003)은 이 법을 ‘불충분하고 결함이 많다’고 평하였으며, Tang(2009)은 ‘여러 결함’을 지적하였고, Chuang(2003)은 ‘허점 투성이’라고 표현하였다), 그 이유로는 모호한 규정(Peng(2003), Tang(2009)), 제한된 범주(Tang(2009)), 포괄적인 감독기구의 결여(Tang(2009))를 들고 있다. 정보이동제약에 관하여 매우 제한적으로 다루고 있는 현 조항들이 시행되고 있는지에 대해서는 알려진 바 없다.

Yuan 총독은 2000년 이후로 이 법을 강화하기 위한 여러 대책을 제안하여 왔지만(Tang(2009)), 아직까지 중앙감독기구 설치 제안은 이루어진 바 없다.

한국

[이 글에서는 다루지 않음]

5. DPA의 독립과 구조에 관한 교훈

5.1. 독립적 기관으로서의 DPA vs. 행정부 소속

일본과 대만의 정보보호체제는 적어도 법률 시행 증거자료의 측면에서 본다면 (호주의 매우 작은 규모의 관할지역인 타스마니아와 노던 테리토리를 제외하면) 아시아-태평양 지역에서 가장 성공하지 못한 사례인 것으로 보인다. 논란의 여지는 있으나 그 주된 이유는 독립적인 정보보호기관의 부재인 것으로 생각된다.

독립적 감독기구는 1995년 EU 사생활보호 지침 이후로 거의 모든 정보보호 국제협약과 기준에서 주요 요소로 등장하였다. 일본의 삶의질 정책 위원회는 일본도 그러한 방향으로 나아가야 할 필요가 있다고 피력함으로써 독립적 기구의 필요성을 인정하고 있는 것으로 보인다.

아시아-태평양 지역에서 적극적이며 가시적인 효과를 거두고 있는 정보보호체제는 뉴질랜드, 홍콩, 빅토리아(주), 뉴사우스웨일즈(주), 호주(연방)의 예와 같이 모두 독립적 DPA를 포함하고 있다. (아직 개시하지는 않았으나) 퀸즈랜드의 경우도 그러하며, 마카오도 의도한 바대로 진행된다면 이 예에 해당한다.

먼저 열거한 10가지 독립성 지표 중에서, 위 5개의 DPA는 다음 요소들을 공유하고 있다.

- 법적 근거
- 타 기관의 지시로부터 자유롭게 조사할 수 있는 권한
- 정해진 임기로 감독관 선임 (단, 뉴사우스웨일즈의 경우에서와 같이 재임이 남용될 가능성도 있음)
- 명시된 부적절한 행동에 대해서만, 그리고 일반적으로 의회에 의해서만 감독관 해임 가능
- 최소한 연례보고서를 통해, 그리고 때로는 특별보고서를 통해 국민과 의회에 직접 보고할 수 있는 권한

- 사적 소송에 대한 면책권

그러나, 아시아-태평양 지역의 독립 DPA에게 독립성을 의미하는 다음과 같은 중요한 속성들은 결여되어 있다.

- 행정부가 아니라 의회에 의한 임명
- 행정부의 관여 없이 결정되는 자원
- DPA 임기 종료후 보장되는 직책
- 타 직책의 겸임 금지

이 조사를 통해 볼 때, 처음 6가지 독립성 지표는 아시아-태평양 지역의 성공적인 정보보호기관에서 기대할 수 있는 특성이라고 볼 수 있다.

5.2. 공공부문과 민간부문의 DPA - 합동 또는 통합기구?

독립성과 관련된 이 10가지 요소들은 민간부문 조직을 조사하는 DPA에 대해서 만큼 또는 심지어 그 이상으로 공공기관의 활동을 조사하는 DPA에게도 분명하게 적용된다. 정부기관은 국민 감시라는 자체 권한을 보호하고자 하는 욕구가 크고 그러한 감시 기능의 수행을 조사하거나 제한하려는 DPA의 시도에 반대하는 경향도 크다. 따라서, 행정부의 권한이 DPA의 적절한 조사를 막기 위해 사용되지 못하도록 하는 것이 중요하다. 이러한 점에서, 'DPA가 공공부문과 민간부문 조사와 관련하여 독립적이어야 한다면 각 부문에 별도의 DPA가 설치되어야 한다는 주장은 합리화될 수 있는가?'라는 또 다른 질문이 제기된다.

Georges(2009)가 주장한 바와 같이, 양 부문의 기술 및 업무 유사성과 두 부문간 정보이동의 증가 현상은, 양 부문의 규제에 있어 일관성을 유지하는 것이 바람직함을 보여주며, 이러한 일관성은 양 부문에 대한 규제 권한이 있는 DPA가 가장 잘 확보할 수 있다. 덧붙여 말하자면, 양 부문에 적용되는 정보보호 원칙들이 대체로 동일해야 한다면 이러

한 원칙을 해석하는 일관된 기구가 필요하다는 점도 단일 DPA의 타당성을 뒷받침한다고 볼 수 있다.

비용 효율성의 문제도 동일한 결론으로 이어진다. 유럽에서는 이러한 사항들을 고려하여 공공부문과 민간부문에 대한 관할권을 통합하는 단일한 국가 DPA를 설치하였다. 아시아-태평양 지역의 뉴질랜드, 홍콩, 마카오, 호주(연방)에서도 같은 결론에 도달하였으며, 이러한 통합은 캐나다와 남아메리카에서도 선호되는 모형이다. 일본, 대만, 한국에서만 DPA 기능의 관리 책임을 여러 부서가 분담하고 있으며, 공공부문과 민간부문에 대해 상이한 모형이 적용되고 있다. 이 지역 외에서는, 미국만이 그러한 접근법을 택하고 있으며, 이를 가리켜 '부문별(sectoral)' 규제라고 부른다.

5.3. 단독 감독관(sole Commissioner) vs. 다수 위원의 감독기구 (multi-member Commission)

유럽과 달리, 아시아-태평양 지역의 국가들은 다수 위원(또는 '합의체(collegiate)') 모형이 더 광범위한 인권위원회를 통해 낯설지 않은 모형인데도 불구하고, 그러한 형태의 DPA를 운영한 경험이 전무하다. 합의체 위원회는 단독 사생활보호/정보보호 감독관 체제에 비해 정치인, 권력 기관, 주요 로비집단의 압력에 저항하거나 자원 감축에 반대하기가 더 용이할 수 있다.

5.3. 단일한 정보보호기능 vs. 기타 기능과 결합

캐나다의 지방 자치구는 사생활보호감독관과 FIO담당관의 통합을 선구적으로 추진해 왔으며, 이러한 통합 현상은 현재 호주(노던 테리토리, 퀸즈랜드의 신설법, 연방 관할권에서 현재 시행중, 뉴사우스웨일즈에서도 가능성 큼)에서 점차 확산되고 있다.

DPA가 정부정책과 입안에 영향력을 행사하고 정보보호 내용이 적절하게 감안되도록 하는 데 있어 중요한 역할을 하며 때로는 정부 정책에 반대하기도 한다는 점을 감안하면, DPA/사생활보호감독관과 옴부즈맨의 병합은 다소 어울리지 않는 조합일지도 모른

다. 그러나, 옴부즈맨의 역할은 일반적으로 행정 업무(주로, 입안)의 공정성과 효율성을 높이는 데 한정되어 있으며, 옴부즈맨은 대체로 협상을 통해 진정인에게 만족스러운 결과를 이끌어낼 수 있도록 하기 위해, 정책 및 입안 관련 이슈에는 관여하지 않으려고 한다. 이와 관련하여 현재까지 유일한 사례인 타스마니아 옴부즈맨의 경우, 사생활보호 책무와 관련하여 주목할 만한 활동을 벌이고 있지 않아 고무적인 사례라고는 볼 수 없다.

5.5. 더 포괄적인 인권기관의 일부?

아시아-태평양 지역에서는 DPA가 더 포괄적인 인권기관의 일부로 운영된 사례는 없다. 별도의 FOI 담당관을 두고 있지 않은 경우, DPA를 더 포괄적인 구조의 일부로 포함시키는 것이 공공부문과 민간부문으로부터의 압력에서 사생활보호감독관을 더 잘 보호하는 한 방법이다.

6. 권한과 기능- 효과적 규제를 위해 무엇이 필요한가?

DPA의 기능과 권한을 어떻게 가장 잘 분류할 수 있는가? 그리고 정보보호원칙의 준수를 확보하는 데 있어 DPA의 실효성을 어떻게 평가할 수 있는가? 먼저, 이론적 측면에서 이를 검토해 보고, 국제협약과 기준에서 제시하고 있는 최저기준을 살펴보도록 한다. 그 다음으로, 이 지역 정보보호체제의 경험이 실제적으로 그러한 기준에 대해 어떠한 의미를 갖는지, 그리고 기존 체제의 실효성이란 측면에서, 그러한 경험을 살펴보고자 한다.

6.1. 사후적(reactive), 사전적(proactive) 권한과 기능

실제로 DPA는 매우 다양한 업무를 수행하며, 대부분의 경우 이러한 업무 수행을 의무 또는 권한으로 법에서 정하고 있다. 이러한 권한과 기능을 어떻게 분류하는 것이 그에 대한 이해를 높일 수 있을 것인가? 또한, 분류를 하면 하나의 업무가 동일한 범주로 분류된 또 다른 업무를 어떻게 대체할 수 있는 지를 이해하기가 쉬우므로, 특정 체제의 실효성 평가 작업이 용이해질 수도 있다.

기능들은 크게 사후적(reactive) 기능들과 사전적(proactive) 기능들로 나뉠 수 있으며, 이러한 구분은 Bygrave가 사용한 'reactive'와 'anticipatory'라는 개념과 본질적으로 동일하다 (2003:85). DPA는 외부 상황에 대해 (강요되어서든, 아니면 자발적으로든) 대응할 수 있는데, 이는 외부 상황이 DPA의 집행기능에 필요한 자원배분을 결정함을 의미한다. 한편, DPA는 사전적 기능을 수행할 수 있도록 주어진 권한을 활용함으로써, 집행자원의 활용에 있어 우선순위를 정하는 전략적 선택을 할 수 있다. 이행을 담보하기 위한 사후적, 사전적 방법 사이에서 적절한 균형점을 찾는 일이 정보보호체제의 설계에 있어 핵심 사항이다.

사후적 기능과 권한은 다음과 같다.

- 접수된 진정을 근거로 법위반 사실 조사
- 장관/기타 기관의 요청/지시에 따라 진정건 조사
- 법률에 의해 촉발된 상황을 근거로, 또는 장관의 요청에 따라, 사생활보호영향평가(PIA)를 실시하도록 요구
- 정보 관리자의 요청에 따라, 정보보호원칙의 완화 또는 조정 결정
- 산업 기관 또는 장관의 요청이 있는 경우에 한하여 부문별 행동규약(code of conduct) 제정

사전적 기능과 권한은 다음과 같다.

- DPA 주도적으로 ('자체 발의') 법위반 사실 조사
- 원칙 이행을 위해 가처분 명령/법원 명령 요청
- 법위반행위의 형사 고발과 이에 대한 사법조치 요청
- 정보관리자에 대한 감사 실시 및 감사 결과 공표 여부 결정
- PIA 실시 여부 결정 및 PIA 결과 공표 여부 결정
- DPA 주도적으로 부문별 행동규약 제정

Bygrave가 지적한 바와 같이 '실제로는 이러한 사전적, 사후적 감독기능의 구분이 모호한 경향이 많다' (2003:85). 예를 들어, DPA가 감사나 PIA를 실시할 수 있는 조건을 법으로 정할 수도 있고, DPA에게 (자원 활용 여부에 따라) 실시 여부를 결정할 수 있는 재량권이 주어질 수도 있다.

Bygrave는 '가부장적(paternalistic) 관리와 참여적(participatory) 관리 형태'로도 구분하고 있으며, 대부분의 정보보호체제는 이 두 형태를 혼합하여 사용하고 있다고 지적한다 (2003:86).

6.1. 평가 - '대응적 규제(responsive regulation)'의 개념

Bennett와 Raab (2003:207)은 '매우 실효성 있는 정보보호체계(highly effacacious data protection system)'은 특히 '이러한 체제의 개발 초기 단계'에서 '적극적이고 단호한 규제권한'을 필요로 할 뿐 아니라 (원칙과 집행권한 모두에 관한) '강력하고 명료한 법', (정부 수집량 감소를 포함한) '정보관리자의 강한 의지', 민간부문의 사생활보호를 유도할 수 있는 시장 인센티브, '국민들의 적극적인 관심과 태도', 일부 사생활보호증진기술(PET: privacy-enhancing technologies)의 활용을 필요로 한다고 지적한다. 필자는 완벽한 체제를 위해서 필요한 요소들을 요약한 Bennett와 Raab의 의견에 전적으로 동의하지만, 이 글에서는 DPA가 행사할 수 있는 집행력을 포함하여 DPA 기능 수행의 실효성을 어떻게 측정할 수 있는지에 초점을 두도록 한다.

사생활보호 규제의 효과적 이행은 어떻게 측정하여야 하는가? 필자는 시행을 위한 여러 선택방안들이 피라미드 또는 계층구조를 이루고, 그 피라미드의 모든 방안들이 신뢰할 수 있도록 활용되며 다양한 유형의 투명성 및 피드백 메커니즘이 존재함을 전제로 하는 '대응적 규제' 이론을 택하였다. Ayres와 Braithwaite(1992)는 자신들이 고안한 대응적 규제 이론의 주요 내용을 다음과 같이 요약하고 있다.

> 2장에서는, 한편으로는 협력적이면서 다른 한편으로는 강경한 규제 방식은 "상충하는 책무로 인해 그 전략이 서로 잘 들어맞지 않기 때문에 운영에 있어 어긋날

수 있다"는 정책적 문제점을 해결하고자 한다. ... 규제의 목적은 해당 기구가 일련의 제재 체계와 개입주의 정도에 따른 규제 전략 체계를 공개적으로 제시할 때 달성할 수 있는 가능성이 더 크다고 한다. 우리가 묘사하는 규제 설계 요건은, 기관이 다양한 개입 방식을 그 강도가 점점 강해지는 순서로(이와 비교되도록 사용 빈도는 점점 줄어드는 순서로) 두 가지 시행 피라미드를 제시하는 것이다. 규제기관은 업계의 실적에 맞추어 피라미드 위로 올라가며 개입을 강화하거나 피라미드 아래로 내려가며 규제를 완화할 수 있음을 보여줌으로써 규제 목적을 달성하는 데 있어 최고의 성과를 거둘 수 있을 것이다.

끝으로, 그 기관이 택할 수 있는 가장 강경한 시행 방안(시행 피라미드의 최고점)이 강도가 높을수록 이행을 보장하는 데 있어 더 효과적이며 강경한 방안을 취해야 할 필요성도 줄어든다고 한다. 규제 기관은 큰 몽둥이를 들고 있다고 여겨질 때 더 부드럽게 말할 수 있는 법이다.

John Braithwaite와 Christine Parker와 같은 이론가들도, 대응적 규제는 '스토리텔링적 특성(storytelling orientation)'을 갖고 있다고 강조한다. 즉, 시행 피라미드의 각 단계에서 이행과 관련된 이야기들(성공 및 실패 사례 모두)이 규제 시스템의 다양한 이행당사자 집단(규제 대상자, 규제의 수혜 대상자, 규제의 실효성 평가 책임자)에게 전달된다. Braithwaite는 (2007년 1월 캔버라에서 열린 APEC 사생활보호 세미나에서의 연설에서), 대응적 규제를 평가하는 기준의 하나는 그 체제가 성공 사례와 실패 사례에 얼마나 '이목을 집중시킬 수 있는가(bubble up)'이며, 단 이러한 사례들이 대표적인 사례들로 신빙성을 지니며 사생활보호 규제에 적용되어야 한다고 밝힌 바 있다. 모든 단계의 제재 사용 내역은 규제 대상자가, 그리고 사생활보호 위반으로 피해를 입은 소비자나 국민이 열람할 수 있어야 한다. 따라서, 대응적 규제를 위해서는 규제 기관의 결정과 기타 시행 관련 활동의 세부적 내용을 공개하는 것이 필수적이다.

7. 권한과 기능 - 국제기준

DPA에게 주어져야 할 적절한 시행 권한이란 무엇인가와 관련하여 사생활보호 관련

국제협약으로부터 어떠한 안내를 받을 수 있는가?

7.1. OECD의 최저 요건

OECD 가이드라인[5]에서 요구하고 있는 최저 시행 장치는, 개인이 자신의 권리를 행사할 수 있도록 하는 합당한 수단과 적정한 수준의 제재 및 구제를 명시하고 있는 법규다. 자율 규제도 시행 가능하다.

7.2. 유럽이사회 협약 108호와 추가의정서의 강화된 요건

협약 108호(1981)는 처음에는 현재와 유사하였지만, '기본 원칙들에 효력을 부여하는 국내법 규정의 위반건에 대해 적절한 제재와 구제'[6]를 요구할 뿐이어서 그 내용이 훨씬 더 애매하였다.

그러나, 협약 108호의 추가의정서(2001)에는 다음과 같이 상당히 세부적인 내용이 담겨져 있다.

제1조. 감독기구

1. 각 당사국은 이 협약의 제II장과 III장 및 이 의정서에 명시된 원칙들에 효력을 부여하는 자국법의 조치들이 이행되도록 보장할 책임이 있는 1개 이상의 기관을 정하여야 한다.

---

5) 제4부. 국내 이행

19. 제2부와 3부에 열거된 원칙들을 국내에서 이행함에 있어, 회원국은 개인정보와 관련하여 사생활과 개인의 자유를 보호하기 위한 법률, 행정 및 기타 절차나 제도를 수립하여야 한다. 회원국은 특히 다음에 힘써야 한다.
   a) 적절한 국내법 채택
   b) 행동규범(codes of conduct)이나 기타 형태로, 자율 규제를 장려하고 지원
   c) 개인이 자신의 권리를 행사할 수 있는 합당한 수단 제공
   d) 제2부와 3부에 열거된 원칙을 이행하기 위한 조치들을 이행하지 못한 경우에 대해 적정 수준의 제재와 구제 명시
   e) 정보 주체에 대한 부당한 차별이 없도록 보장

6) 제10조 (제재와 구제)
각 당사국은 이 장에 열거되어 있는 정보보호 기본 원칙에 효력을 부여하는 자국법 조항의 위반건에 대해 적절한 제재와 구제를 확립하기 위하여 힘써야 한다.

2. a. 이를 위해, 위 기관은, 이 의정서 제1조의 1항에 언급된 원칙들에 효력을 부여하는 자국법의 조항이 위반된 경우에 법적 절차에 관여하거나 관할 사법당국에 제소하는 권한과 함께, 특히, 조사 및 개입 권한을 지녀야 한다.
   b. 각 감독기구는 개인이 그 기관의 관할권 내에 있는 개인정보 처리와 관련하여 자신의 권리 및 기본적 자유의 보호에 관하여 제기한 진정을 심리하여야 한다.
3. 감독기구는 자체 기능을 완전히 독립적으로 수행하여야 한다.
4. 감독기구의 결정에 대해 진정이 제기되는 경우에는 법원을 통해 항소할 수 있다.
5. 이 협약 제IV장의 조항에 의거하여, 그리고 제13조 조항을 침해하지 않는 범위 내에서, 감독기구는 자체 업무의 수행에 필요한 정도로, 특히 모든 유용한 정보를 교류함으로써 상호 협력하여야 한다.

협약 108호와 그 추가의정서는 현재 기준을 충족하는 비유럽 국가들에게도 가입이 개방되어 있다.

7.3. EU지침 요건과 '적정성(adequacy)' 기준

EU 사생활보호지침에는 주요 요건이 제22-24조(사법적 구제와 제재), 제27조(행동규범), 제28조(감독기구)에 기술되어 있으며, 해설 부분(recitals)의 54항(사법적 구제와 손해배상의 필요성), 61항(행동규범의 타당성), 62항(감독기구의 독립성), 63항(조사권, 소송개입권, 투명한 소송 보장을 지원할 권한)에서 보완하여 설명하고 있다.

EU지침에서 요구하고 있는 EU DPA의 여러 구체적인 특징은 다음과 같다 (Bygrave, 2003:Ch 4).

- 정보보호와 관련된 행정조치나 규정 제정시에 협의 대상이 될 권리 (A 28(2))
- 정보처리사업의 감독, 조사 및 개입 (A 28(3))
- 진정을 심리하고 법위반행위에 관한 소송 개시 (A 28(4))
- 등록이 요구되는 정보처리에 관한, 일반 열람이 가능한 등록부 작성, 유지 (A 18-19)
- '정보주체의 권리와 자유에 특정 위험을 가할 가능성이 있는' 정보처리사업에 대한

'사전확인(prior checking)' 체제를 운영할 수 있는 권한 부여 가능 (A 20)

- 타 DPA와의 협력을 촉진하는 방향으로 권한을 행사할 수 있는 역량 (A 28(6))

Bygrave는 'EU지침은 DPA가 과징금을 부과하거나 손해배상을 명할 수 있어야 하는지에 대해서는 명시하고 있지 않지만 그러한 권한은 분명히 이 지침에 부합한다' (2003: 72)고 논하였다. Bygrave의 주장에 의하면, A 28(3)에 의한 개입권은 그러한 두 가지 방식 중 어느 것으로도 해석될 수 있다.

EU지침에는 직접적으로 DPA와 관련이 없는 이행보장 조항들도 포함되어 있다.

- 정보주체에게는 자신의 정보보호권 침해에 대해 '사법적 구제'가 주어져야 하며 (A 22), 정보주체가 자신의 권리 행사를 위해 법원에 (DPA에 진정을 제출하는 방법이 아니라) 직접 접근하는 것은 허용되지만 강제되지는 않는다 (Bygrave, 2003:78).
- DPA 결정에 대한 항소권이 주어져야 하지만, 법적 문제에 한정되고 사실 관계에 대한 항소는 허용되지 않을 수 있다 (Bygrave, 2003:78).
- 보상 받을 수 있는 권리가 주어져야 하며(A 23(1)), 정보관리자가 그러한 위반에 책임이 없음을 입증할 수 있는 경우에는 예외가 인정되어야 하지만 (A 23(2)), 이 조항이 경제적 손실뿐만 아니라 비경제적 (가령, 정신적) 피해도 포함하는지는 (그럴 가능성이 크지만) 분명치 않다 (Bygrave, 2003: 78).

EU '적정성' 기준

제29조 실무단이 권고한 적정성 평가 방법은 절차 및 시행 메커니즘의 세 가지 측면을 고려하고 있다.[7] 즉, (i) 규칙(정보보호원칙)에 대한 "양호한 수준의 이행" 달성, (ii)

7) 제29조 실무단은 이와 관련하여 다음과 같이 논하고 있다.
"정보보호체제는 본질적으로 다음의 세 가지 목적을 지닌다.
1) *양호한 수준의 규정 이행*을 추진한다 (어떠한 체제도 100%의 이행을 보장할 수는 없지만 이행 수준은 국가마다 차이가 있다). 우수한 제도의 경우에는 일반적으로 정보관리자들의 의무에 대한 인식이 높은 한편 정보주체들의 권리 및 권리 행사 수단에 대한 이해가 높은 것이 특징이다. 효과적이면서도 강력한 제제의 존재는, 행정기관, 감사기구 또는 독립적 정보보호관에 의한 직접적 검증 체제와 마찬가지로, 법규준수를 확보하는 데 있어 중요한 역할을 할 수 있다.

개별 정보 주체가 자신의 권리를 행사하도록 지원 제공, (iii) 규칙이 이행되지 않은 경우에 피해자에게 적절한 보상 제공 여부와 정도를 평가한다.

이 실무단이 효과적인 진정 제도 이상을 언급하고 있다는 사실은 첫 번째 항목에 대해 상술한 내용에서 알 수 있다.

> "우수한 제도의 경우에는 일반적으로 정보관리자들의 의무에 대한 인식이 높은 한편 정보주체들의 권리 및 권리 행사 수단에 대한 이해가 높은 것이 특징이다. 효과적이면서도 강력한 제제의 존재는, 행정기관, 감사기구 또는 독립적 정보보호관에 의한 직접적 검증 체제와 마찬가지로, 법규준수를 확보하는 데 있어 중요한 역할을 할 수 있다."

이러한 일반적 기준은 위에서 기술한 EU내 DPA에 대한 보다 구체적인 요건의 측면에서 이해되어야 할 필요가 있는데, 이러한 기준과 비교하여 제3국 집행체제의 '적정성'을 제29조 실무단의 세 가지 기준에 의해 간접적으로 평가하여야 하기 때문이다.

7.4. DPA 국제협회 인정 요건

DPA 인정과 관련하여, DPA 국제협회(International Privacy Commissioners)는 OECD와 마찬가지로 일반론적인 수준에 그치고 있지만, 논평을 통해서 '적절한 범위의 기능'에 해당하는 것과 그렇지 않은 것을 밝히고 있다.

> 4. 적절한 기능
>
> DPA는 적절한 범위의 기능과 함께 그러한 기능을 수행하기 위해 필요한 법적 권한을 지녀야 한다.

---

2) *개별 정보주체의 권한 행사를 지원*한다. 정보주체는 자신의 권리를 신속하고 효과적으로, 그리고 비용 부담 없이 행사할 수 있어야 한다. 이를 위해서는, 진정건에 대한 독자적 조사를 허용하는 제도적 장치가 마련되어야 한다.

3) 규정이 위반된 경우 피해당사자에게 *적절한 구제*를 제공한다. 이는 핵심 요소로서 적절한 경우 보상 지급과 제재부과가 허용되는 독자적인 심판 또는 중재 체제를 포함하여야 한다.

해설: DPA는 이행, 감독, 조사, 시정, 지도 및 대국민 교육과 같은 분야에서 다양한 기능을 갖게 된다. DPA는 단순히 자문기구에 그쳐서는 안 되며 법적 또는 행정적 결과를 수반하는 감독권한을 지녀야 한다.

7.5. DPA 국제협회의 기준안(2009)

이 국제협회에서 현재 개발중인 기준은 '정보 주체가 제기한 진정을 처리할 수 있고 이행을 보장하기 위해 필요한 경우에 조사와 개입이 가능한 정도의 충분한 권한과 적정 수준의 자원'과, 그러한 권리를 강행하기 위해 법원에 제소할 수 있는 권한을 포함할 것으로 보인다[8].

7.6. APEC 사생활보호 기본틀(APEC Privacy Framework)의 기준 부재

이 기본틀의 제IV부 Section A ("국내 이행을 위한 지도")의 I-IV에 명시되어 있는 이행 관련 부분은 극도로 비규정적(non-prescriptive)이다. 회원국은 '불필요한 정보이동 장벽'을 파악하고 제거하거나 피하기 위한 '모든 필요하고 적절한 조치를 취하여야 한다고 명시하고 있지만 (I), 사생활 보호를 위한 '모든 필요하고 적절한 조치'를 취하도록 하는 비슷한 수준의 강력한 명령은 포함하고 있지 않다. 확실히 편향되어 있다.

이 기본틀에서는 사생활보호 원칙의 이행을 위한 특정 수단을 요구하고 있지 않으며, 대신 국가간 양립성(compatibility)라는 총체적 목적 하에서 기본틀 이행 수단은 국가(APEC에서는 'Member Economies'로 표현함)에 따라 상이할 수 있으며 원칙별로 다양할

8) 22. 모니터링
1. 모든 국가에는 국내법에 의거하여, 이 문서에 명시된 원칙들의 준수를 감독할 책임이 있는 1개 이상의 감독기구가 존재하여야 한다.
2. 이 감독기구는 공평성, 독립성, 기술적 적격성을 보증하여야 하며, 정보 주체가 제기한 진정을 처리하고 개인정보처리와 관련한 사생활보호에 관한 국내법의 이행을 보장하기 위해 필요한 경우 조사를 실시하고 개입할 수 있는 충분한 권한과 적정 수준의 자원을 갖추어야 한다.
3. 어떠한 경우라도, 2항의 감독기구 업무의 대상이 되어야 하는 사항에 대한 사법적 검토를 저해하지 않는 한, 정보 주체는 관련 국내법에 명시된 규정에 의한 자신의 권리를 행사하기 위해 법원에 제소할 수 있다.

수 있다고 기술하고 있다 (II).

위의 (II) 부분은, APEC에서는 법률의 지원을 받지 않는 완전한 자율 규제에서부터 법률에 근거한 사생활보호 국가기관에 이르기까지 다양한 수단이 용인된다는 점을 분명히 하고 있다.

> '이 기본틀에 효력을 부여하고 개인의 사생활보호를 보장하는 방법은 여러 가지가 있는데, 이 기본틀에 의해 권리를 행사할 수 있도록 하는 법률적, 행정적 방안 또는 업계의 자율적 규제를 실시하거나, 또는 이러한 여러 방법들을 절충하는 것이다.'

> '실제로, 이 기본틀은 회원국이 적절하다고 판단하는 다양한 이행 방법을 수용하여 유연한 방식으로 이행될 수 있다. 중앙당국, 복수 기관으로 구성된 집행 기구, 지정된 산업 기구 네트워크 또는 이러한 여러 기구를 통합한 조직을 통해 이행할 수 있다.'

진정인이 '그러한 위반으로 인해 개인에게 가해진 실제적 또는 잠재적 피해의 정도에 상응'하는 구제를 선택할 수 있도록 하는 것이 중요하다는 내용도 있다 (V).

입법이 구제를 제공하는 한 수단으로 언급되고 있기는 하지만, 입법이 요구되거나 심지어는 권고되고 있지도 않다 (V). 이와는 대조적으로, OECD 가이드라인은 '제4부 - 국내이행'에서 '회원국은 적절한 국내법'(OECD 19(a))과 '개인이 자신의 권리를 행사할 수 있도록 합당한 수단'(19(c)), '적정 수준의 제재와 구제(정보수출 위반에 대한 제재 및 구제 포함)'(19(d)), '부당한 차별이 이루어지지 않도록 하는 수단'(19(e))을 포함하여 다양한 기타 수단을 채택하도록 각별히 힘써야 한다고 적고 있다. 입법에 대한 OECD 지지도 미온적 수준이지만, APEC의 경우에는 그러한 지지가 전무하다.

7.7. 최저 국제요건에 관한 결론

APEC 사생활보호기본틀은 정보보호원칙의 이행을 보장하기 위한 뚜렷한 최저오견을 정하고 있지 않다.[9] 대부분의 다른 국제협약과 기준(OECD 가이드라인(1981), 유럽이사회(CoE) 협약(1981), 국제정보보호기구협회(IPC) 인정기준 및 기준안(2009))은 요건에 대

해 간략하면서도 일반적인 내용을 담고 있지만, 충분한 조사권, 적절한 구제, 법원 접근권과 관련된 사항들은 포함하고 있다. 세부적인 내용을 담고 있는 기준은 EU 사생활지침(1995)과 유럽이사회 협약 선택의정서(2001) 뿐이다. 따라서, 한 국가가 자국의 정보보호체제가 유럽 기준에 부합하거나 그러한 기준에 비추어 '적정'하다고 간주되는 것이 바람직하다고 여기는 경우에는 최저 요건을 결정하기가 훨씬 수월하겠지만, 그렇지 않다면 상세한 최저 요건이 마련되어 있다고 말하기는 어려울 것이다.

다양한 국제협약과 기준에 명시되어 있는 DPA의 권한과 의무는 다음과 같다.

- 조사권 (CoE 의정서, EU지침, IPC기준안)
- 적어도 조정(mediation)의 형태로 개인 또는 대표집단에 의한 (EU지침) 진정건을 '심리'할 수 있는 권한 (CoE 의정서, EU지침, IPC기준안)
- 정보보호원칙의 위반에 관한 소송에 관여하거나 위반사실을 법원에 제출할 수 있는 권한 (CoE 의정서, EU지침)
- DPA 결정에 불복하여 법원에 항소할 수 있는 (양 당사자에게 주어진) 권리 (CoE의정서, EU지침)
- (i) 정보처리 전 개입 (EU지침), (ii) 정보처리 금지 및 중단 (EU지침), (iii) 정보처리 감독 (EU지침), (iv) 관련 사안을 정치적 기관에 회부 (EU지침) 등의 권한을 포함하는 실효성 있는 조사권 (EU지침, IPC기준안)
- 타 DPA와 협력할 수 있는 역량 (EU지침, CoE의정서)
- 정기적인 업무 보고 요건 (EU지침)
- 통보 의무가 있는 정보처리활동에 대한, 일반인의 공개 열람이 가능한 등록부 작성, 유지 (EU지침)
- 법적 권한을 지닌 적절한 기능 (IPC 인정요건, IPC기준안)

위의 국제협약과 기준은 (반드시 DPA의 기능은 아닌) 감독기능과 구제에 관한 추가로

9) APEC의 'Pathfinder' 프로젝트를 통해 최저요건을 추진할 가능성도 있지만, 아직까지는 불투명하다. Greenleaf(2009)와 Waters(2008) 참조.

명시하고 있다.

- 법령에 구체화된 구제방안 (OECD)
- 권한 행사를 위한 법원 접근성 (IPC 기준안)
- 자율규제 촉구 (OECD)
- 합리적인 권한행사 수단 (OECD, IPC 기준안)
- 적절한 제재 및 구제 (OECD, CoE)
- 정보주체에 대한 부당한 차별이 없도록 보장 (OECD)

이러한 국제협약과 기준의 초점은, EU지침의 경우에는 부분적으로 예외라 할 수 있지만, 주로 이행보장의 사전적 측면이 아니라 사후적 측면에 주어지는 경향이 크다.

8. 권한과 기능(의 부재) – 지역적 경험

아시아-태평양 지역의 국가가 정보보호의 이행을 보장하기 위한 '기준'을 마련할 수 있는 또 다른 중요한 방법은, 이 지역의 다른 국가 및 DPA의 경험을 참고하는 것이다. 단순히 관련법령에서 어떠한 권한과 책무를 부여하고 있는가를 살펴보는 것만으로는 충분치 않고 (이를 통해 실질적 기준을 평가할 수는 있지만), 그러한 권한과 책무의 실효성(과 역량)도 평가하여야 한다. APEC 사생활보호기본틀이 이러한 사항에 대해 어떠한 유용한 내용도 포함하고 있지 않다고 해서 이 지역이 어떠한 경험도 없는 것은 아니다[10].

이 글에서 12개 관할권(호주의 여러 주와 자치구 포함)의 이행체제의 모든 측면을 상세하게 논하기는 불가능하지만, 각 체제의 가장 독특하고 흥미로운 일부 부분은 바람직하거나 부적절한 관행의 사례로 살펴볼 수 있을 것이다.

10) APEC 기본틀의 정보보호원칙에 관한 유사한 주장과 얼마나 이 기본틀이 아시아-태평양 지역의 실질적 기준을 충분히 보여주고 있지 못한가에 대한 내용은, Greenleaf(2009)를 참조.

8.1. 홍콩 – 구제책의 부재

홍콩의 법령(Ordinance)에 명시된 진정인의 권리구제와 감독관(Commissioner)의 집행력은 모두 부적절하다.

감독관은 위반이 의심되는 사안을 조사하고 시정명령을 내릴 수 있는 권한을 통해 법령의 요건을 집행한다 (ss. 38~50). 이러한 조사권은 자신의 개인정보와 관련하여 위반사실을 주장하는 개인의 진정에 의해, 또는 감독관이 자발적으로 행사할 수 있다 (s. 38). 감독관은 처리기관의 구내 출입 권한(s. 42(1))과 자료제출 요구권(s. 44)을 포함하여 방대한 조사권한을 지니며, 진정 처리 결과를 보면 이러한 권한은 간혹 (드물게) 사용되고 있다.

위반사항에 대한 부적절한 제재

감독관은 조사 실시 후에, 정보사용자가 법령의 요건을 위반하였으며 그러한 위반이 지속되거나 반복될 가능성이 높다고 판단하면, 정보사용자에게 시정에 필요한 조치를 취할 것을 지시하는 시정명령을 내릴 수 있다 (s. 50).

원칙을 위반하는 것은 그 자체로 형사상 위법 행위가 아니지만, 시정 명령의 위반과 같이 법령에 명시된 기타 요건을 위반하는 것은 위법 행위다(s.64와 s.62(10)). 따라서, 사생활보호감독관은 시정 명령에 함축되어 있는 형사상 제재 가능성을 이용하여 원칙이 이행되도록 할 수 있다 (s.50). 그러한 명령을 이행하지 않는 것은 위법 행위다 (s.64(7)). 이 명령서에는 위반을 시정하기 위해 필요한 조치들이 명시될 수 있다. 시정 명령이 실효성에 있어 지니는 한 가지 큰 제약은, 해당 정보 사용자가 그러한 위반 행위를 지속하거나 반복할 가능성이 있는 경우에만 발부된다는 점이다 (s.50(1)(b)). 시정 명령은 정보사용자에게 '위반 행위를 시정하기 위해 해당 명령서에 명시된 조치들을 취하도록' 지시할 수 있다 (s 50(1)(b)).

따라서, 시정 명령은 지속되거나 예상되는 위반 행위로부터 다른 정보 주체들을 보호하는 데는 유용하지만, 해당 진정인에게 제공되는 구제는 제한적이다. 위반 행위가 정보

사용자의 관행에 있어 어떠한 체계적인 결함 때문은 아니고 그럼에도 불구하고 이미 진정인의 명예 훼손, 감정적 상처 또는 재정적 손실을 야기하였다면, 시정 명령에 의해 제공되는 구제는 동일한 위반 행위의 재발 또는 지속이 방지된다는 것뿐이며, 그러한 위반 행위가 발생할 가능성이 없다면 시정 명령은 결코 발부되지 않는다.

향후 위반을 억제하기 위한 한 방편으로, 시정 명령 불이행시 사법처리하는 것도 그다지 유용하지 못한데, 그러한 경우가 너무 드물 뿐 아니라 그로 인한 벌금이나 기타 처벌이 미약하기 때문이다.

작동하지 않는 보상 규정

사생활보호감독관(구제 권한은 거의 없고 보상을 부여할 권한은 전혀 없음)에게 진정을 제기할 수 있는 권한을 제외하면, 개인이 이용할 수 있는 유일한 구제책은 법령(Ordinance) s. 66에 명시된 법원에서의 조치를 통하는 방법이다. 진정인은 DPP의 위반을 포함하여 법령의 위반으로 인해 발생하는 감정적 상처를 포함한 피해에 대해 보상을 받을 수 있는 법적 권리가 있다(s. 66). 정보 사용자는 위반하지 않기 위해 합당한 주의를 기울였음을 입증할 수 있거나 제3자로부터 입수한 부정확한 정보로 인해 위반한 것이라면 그것으로 자신을 충분히 변호할 수 있으며, 따라서 보상은 진정인에게 가해진 피해가 아니라 정보 사용자의 유죄 여부에 따라 결정된다.

그러므로, 개인이 보상을 받기 위해서는 홍콩 법원에서 민사소송을 개시하여야 하는데, 소송에 실패하는 경우 (홍콩의 통상적 관행에 따라) 양 당사자가 소송 비용을 부담하여야 하는 위험이 항상 존재하며, 익명성도 보장되지 않는다. 사생활보호감독관은 그러한 소송에서 개인을 지원할 수 없으며 (차별건의 경우에 대한 홍콩의 관행과는 대조적임), 위반에 관한 s 48 보고도 허용되지 않는다. 진정 내용은 처음부터 새로이 입증해야 한다. 지금까지 s 66에 의한 진정에 성공한 사람은 없으며 법원에 제소된 중대한 사건도 없었다 (한 번의 시도가 있었으나 잘못된 판단에 의한 것으로 기각되었다). 그 이유를 이해하기는 어렵지 않다. 상당한 부유층이 아닌 자가 제기한 사생활보호 관련 진정에 대해서 이 보다 더 비호의적인 곳은 찾아보기 어려울 것이기 때문이다.

홍콩이 s. 66 관련 진정을 억누르는 분위기에 있기는 하지만, 이러한 진정이 극소수에 이른다는 점은 이해하기 어렵다. 자신의 치부를 드러낸다는 것이 중국 문화에서는 받아들여지기 힘든 일이지만, 홍콩은 아시아의 기준에서 본다면 상대적으로 소송하기 좋아하는 사회이며 '잘못된 혐의'가 주어지면 자신의 명예를 지키기 위해 명예훼손 소송을 거는 일도 흔하다. 아마도 소송인과 변호사들이 사생활보호법도 자신의 명예를 지키기 위해 활용될 수 있다는 점을 인식하고 있지 못한 듯하다.

사생활보호감독관은 보상의 지급으로 분쟁 해결을 중재하는 것이 자신의 역할의 일부라고 여기고 있지 않은 듯하며, 보상금 지급은 사생활보호감독관이 중재한 진정건 보고서에 언급되어 있지 않다. 사생활보호감독관은 보상금의 지급을 요구할 권한이 없으며, 당사자들이 상호 만족스러운 결과에 도달할 수 있도록 조정하는 구체적인 기능도 없다. 진정 당사자간에 비공식적 해결을 보여주는 사례들이 일부 있으나, 사생활보호감독관실이 밝힌 바에 의하면 보호관이 조정을 하지는 않고 단지 당사자들이 협상하도록 일임할 뿐이며, 자발적으로 보상금이 지급되었는지에 대해서는 알고 있지 못한다고 한다 (Lam, 2005). 보상이나 손해배상금 지급을 언급하는 진정건은 보고된 바 없다. 따라서, 진정인이 s 66에 의한 보상을 받기 위해서는 자신의 자원을 이용하여야 하는 것으로 보인다.

따라서, 홍콩의 정보보호법이 시행된 지 거의 10년이 되었지만 보상금으로 1달러라도 받았다는 기록이 전혀 없다. 이는 한국의 경우와 상당한 대조를 이루는 현상으로, 한국에서는 위반 사실이 입증되면 보상금 지급이 일반적으로 이루어지기 때문이다. 또한, 호주, 뉴질랜드, 캐나다의 관행과도 차이를 보이는데, 이 세 나라에서는 (아직까지 일반적이라기보다는 예외적이지만) 보상금 지급이 명령과 해결의 한 요소다.

법령에 의하면 사생활보호감독관은 진정인을 지원하기 위해 s. 66 진정건에 개입할 수 있는 권한이 없으며, 손해배상을 요구할 수 있는 권한도 사생활보호감독관이나 AAB에 주어져 있지 않다. 이에 상응하는 호주와 뉴질랜드의 기구들은 그러한 권한을 지니고 있다. 개인 구제의 실효성 측면은 홍콩 제도의 가장 취약한 부분의 하나임이 분명하다.

개인은 DDP의 이행을 위해 기존의 또는 예정된 관행을 금지하는 가처분명령을 내리도록 법원에 직접 제소할 수 있는 권리가 없으며, 다만 사생활보호감독관에게 진정을 제출할 수 있다. 법원의 가처분명령을 요청하는 권리는 타 국가에 존재하는데, 한 예로 호주의 1988년 사생활보호법 s. 98에 명시되어 있다.

진정 - 항소권과 심사권

사생활보호감독관이 진정건을 조사하지 않거나 진정건을 조사한 결과 시정명령을 발부하지 않겠다고 결정을 내리는 경우, 진정인은 그러한 진정에 맞서 준사법 법정 기구인 행정심판국(Administrative Appeals Board (AAB))에 항소할 수 있다. 마찬가지로, 정보 사용자는 사생활보호감독관의 시정명령 발부 결정에 대해 AAB에 항소할 수 있다 (s.47(4)). AAB의 판정에 대해 법원에 항소할 수는 없지만, 불만스러운 당사자는 AAB 판정에 대해 사법적 심사를 요청할 수 있다. AAB의 판정에 대한 심사를 요청한 개인에게는 '법정에서의 발언 기회(day in court)'가 주어지며 이 경우에 개인에게 비용이 부과될 가능성은 거의 없지만 보상이나 기타 구제는 이루어지지 않는다.

항소할 수 있는 통로도 부족하고, 사법적 심사도 드물고, 심지어 AAB 판정도 많지 않다는 점은, 이 법령에 대한 사법적 또는 준사법적 해석도 많지 않음을 의미한다. 감독관과 소속 직원들은 법령에 대한 자신들의 해석이 정확하다는 전제 하에서 행동해야 하지만, 어느 곳에서든지 사생활보호법에 관한 사법적 결정은 예측 불가능하다는 점이 지나치게 낙관적인 태도를 낳는 것으로 보인다. Eastweek건이 바로 그러한 증거다. 따라서, 홍콩의 사생활보호법의 의미는 더 많은 사법 판결이 내려지기 전까지는 전반적으로 매우 불명료한 상태로 남게 될 것이며, 감독관실의 법 해석이 실질적인 법의 역할을 계속하게 될 것이다. 감독관실은 DDP의 의미와 법령의 기타 주요 사항을 자체적으로 상세하게 해석하여 발간하였으며 (HKPCO 2006), 이는 이례적이면서도 가치 있는 일이다.

집행관련 조항에 대한 검토 (2009)

홍콩 정부의 '헌정 및 대륙사무국(Constitutional and Mainland Affairs Bureau)'은 '개인

정보(사생활) 법령의 검토에 관한 협의서(Consultation Document on Review of the Personal Data (Privacy) Ordinance)' (2009년 8월)를 공표하여, 2009년 11월 30일까지 의견을 제출하도록 요청하였다. 이 협의서에서 제기한 안건들은 다음과 같다.

- 감독관은 s. 66에 따라 보상을 원하는 진정인에게 법적 지원을 제공할 수 있어야 하는가?
- 감독관은 보상을 재정할 수 있어야 하는가?
- 정보보호원칙의 위반은 위법 행위로 간주되어야 하는가?
- 정보보호원칙의 상습적 위반은 위법 행위로 간주되어야 하는가?
- 상습적 위법의 경우 더 과중한 제재를 가하여야 하는가?

현재 검토중인 사안들은 홍콩 법령의 집행 측면에 대한 불만 수준을 보여주는 좋은 척도가 된다.

8.2. 마카오 – 더 다양한 구제방안

마카오의 개인정보보호법(2006)은 (홍콩 법령의 영향을 받았다는 평가도 있지만) 많은 부분에서 포르투갈의 법률과 매우 유사하다. 결과적으로, 마카오의 법은 아시아의 다른 정보보호법보다는 오히려 1005년 EU 사생활보호 지침에 더 가깝다.

개인정보보호국(Office of Personal Data Protection (OPDP))은 EU와 유사한 정보보호법이 중국 사회에는 매우 낯설기 때문에 신중하게 시행할 필요가 있다는 입장에서 초기에 대국민 홍보에 주력하였다. 많은 마카오 사람들이 아직 이 법을 잘 알지 못하지만, ODPD는 이 기구가 운영된 지 거의 2년이 지난 지금 마카오의 공공 및 민간부문 기관 대부분이 이 법에 대해 알고 있으며 이 법을 위반한 경우에는 행정적 제재나 심지어는 형사 혐의로 처벌될 수 있다는 점도 알고 있다고 평가하고 있다.

이행 조치

다양한 시행 대책들이 마련되어 있다. 개인은 OPDP에 진정을 제기할 수 있으며, 또한

기타 법률적, 행정적 구제를 요청할 수도 있다. 개인정보보호법 위반으로 피해를 본 사람은 해당 정보 관리자가 그러한 피해에 대한 책임이 없음을 입증하지 않는 한 그 관리자로부터 보상을 받을 권리가 있다 (14조). 여러 유형의 위반에 대해 다양한 민사상 (행정적) 위법 행위로 정하고 있으며, ODPD는 그러한 경우에 벌금을 정하는 역할을 한다. 수집 목적과 일치하지 않는 목적으로 개인정보 사용, 무단 정보 매칭, 기타 중대한 위반 행위는 형사상 위법 행위로 명시하고 있다. '공개적 경고(public warning)와 비난(censure)', (위반 행위에 관한) '판결문 공개'는 '추가적 처벌'이며, 정보의 처리와 말소 금지도 마찬가지다. 중요한 성격의 기본권이 침해된 경우에는, 상고법원(Court of Final Appeal)에 직접 항소할 수 있다.

시행 규정은 복잡하기 때문에 위에서 요약한 내용만으로는 충분치 않다. 마카오의 법은 적어도 이론적으로는 아시아-태평양 지역의 정보보호법 중에서 가장 포괄적인 '시행 피라미드(enforcement pyramids)'를 갖춘 법이라고 말할 수 있다. 문제는 '그 법이 어떻게 활용되고 있는가?'에 있다. 그러나, '이 질문에 답하기에는 너무 이르다'. OPDP는 담당 사건에 관하여 요약한 내용을 중국어와 포르투갈어로 발간한 연례보고서에 포함시키고 있으며, 2007년부터는 영어로도 제작된 웹사이트에 일부 판정문 요약본을 싣고 있다 (OPDP website, 2009). 지금까지 보고된 사건들 중에서 보상금 지급이 이루어진 예는 없다.

통보/등록제도

개인정보보호법은 (일부 정보처리에 한하여) 준등록 제도(quasi-registration system)를 명시하고 있는데 이는 아시아-태평양 지역에서 이례적인 경우다. 대부분의 자동 정보처리 또는 민감한 정보의 처리는, 적용 예외 승인을 받은 경우는 제외하고, 8일 내에 OPDP에 통보하여야 한다 (21조). 민감한 정보의 처리 (일부 경우), 신용 정보, 정보 매칭 또는 부차적 목적을 위한 정보 사용에 대해서는 '사전 검증(prior checking)' (즉, 인가)이 요구된다. 통보 비용은 없다. 통보와 인가 내용은 공개 명부(public register)로 발간되고, 마카오의 개인정보처리의 여러 측면을 다루고 있는 OPDP 연례보고서에 포함되어야 한다.

감시 및 고용서비스 분야에서 OPDP는 이미 통보/등록 절차를 개시하였다 (주로 21조

에서 다루고 있지만 경우에 따라서는 22조와 기타 조항에서도 다루고 있음). 일반 기업뿐만 아니라 정부부처, 은행, 공공기관, NGO를 대상으로 하는 설명회를 개최한 결과, 현재 이들 중 상당수가 통보를 해오고 있다. OPDP는 통보/등록제도를 몇 년 이내에 본격적으로 실시할 예정이다 (2008년 홍콩에서 개최된 29차 APPA 포럼에서 발표한 내용). 1단계로 공공부문에서 실시한 후에 민간부문으로 확대할 계획이다. 약 2년이 소요될 것으로 추산하고 있으며, 그 이후에 통보에 관한 구체적인 규정을 수립할 것이다. 이후에는 적절한 통보 없이 정보를 처리하는 경우에 제재가 가해질 것으로 보인다.

8.3. 호주연방감독관 – 활용되지 않는 권한과, 항소 제도

호주의 1998년 연방사생활보호법(Privacy Act)은 대응적 규제에 실패한 또 다른 사례로 볼 수 있다. 이론적으로는 사생활보호감독관에게 적정 권한이 주어져 있지만, 다양한 이유에서 이러한 권한이 전혀 사용되고 있지 않다 (그리고 진정인들도 항소를 제기할 수 없다). 이러한 사실이 정보관리자에게 전달하는 메시지는, 사생활보호법을 무시하더라도 자신의 사업에 악영향이 미칠 위험은 낮다는 것이다.

개인은 IPP나 NPP (또는 세금 문서 번호, 신용 보고 등에 관한 기타 구체적인 정보보호 원칙 - 뒤에서 다시 논의함)의 위반에 관하여 OPC에 진정을 제출할 수 있다. 연간 평균 1,250건에 대한 조사가 이루어지는데, 그 중 2/3는 민간부문 규정의 적용을 받는다.[11] 감독관은 조사를 실시할 수 있는 광범위한 권한을 지니지만, 사용되는 경우는 드물다. 진정인은 먼저 해당 정보 관리자와 문제를 해결하기 위한 노력을 기울여야 할 의무가 있다. 대부분의 진정건은 조사와 조정(mediation)의 절차에 따라 처리되지만, 그렇지 않은 경우에는 감독관이 강제적인 '결정(determination)'의 권한 행사를 고려하게 된다.

진정건 처리 결과에 대해 상세한 내용이 발표된 경우는 거의 없다. 2003년 이후로 감독관은 결정을 내리기 전에 해결된 주요 진정건을 익명으로 요약하여 그 내용을 공표하

11) OPC, supra n. 32, p. 126. By contrast, complaints relating to breach of IPPs counted for only 17% of total complaints closed during the period 1.7.2003.30.6.2004: see OPC, The Operation of the Privacy Act Annual Report: 1 July 2003 . 30 June 2004 (OPC, Sydney, 2004), section 5.4.2, p. 55.

여 왔으며, 이러한 진정건은 평균 연간 15건에 이른다.

이 법에 의해 감독관은 필요한 경우 법적인 조사권을 이용하여 “자체 발의 조사(own motion investigation)”를 실시할 수 있으나, 그 결과로서 집행력 있는 결정을 내릴 수는 없다. 이 법에서는 한 진정인이 진정인 집단을 대표하여 대표 진정을 할 수 있도록 허용하고 있으며, 이 경우에는 해당 집단의 모든 구성원에게 유리한 집행력 있는 결정으로 이어질 수 있다. 유일하게 발표된 사례는 소비자 NGO가 진정인 집단을 대표한 경우인데, 그 결과로서 지금까지 유일하게 민간부문 기관에 불리한 결정이 내려진 것은 결코 우연이 아닐 것이다.

그러나, 감독관은 조정이 실패한 경우에 손해배상을 지시하거나 사과나 구제조치를 요구하는 ‘결정’을 내릴 수 있는 광범위한 권한이 분명 있다. 이러한 결정권은 지난 16년간 사생활보호법이 시행되는 동안 단 여덟 번 사용되었다 (그리고 그 중 네 번은 동일한 분쟁에서 사용되었다). 이것이 진정의 성공적인 해결을 의미하는 것인지에 대해서는 의견이 분분하지만, 결정문이 내려지지 않았기 때문에 공공부문과 민간부문 모두 위반을 하더라도 어떠한 불리한 결과가 발생하지 않으므로 법을 무시해도 좋다는 인식을 갖게 되었다는 견해가 더 설득력이 있다. 익명 결정문은 감독관이 공표한다.

감독관의 결정에 대한 항소 부재

행정적, 사법적 권한의 분리에 관한 헌법상 이유로 인해, 감독관의 결정은 해당 사안이 법원에서 처음부터 다시 재심리를 거치지 않으면 (법원의 심리에서 감독관의 판단이 ‘일단 채택되는 증거(*prima facie* evidence)’임에도 불구하고) 해당 정보 관리자에 대해 불리하게 강행할 수 없다. 감독관은 결정의 이행을 요청할 수 있다.감독관의 결정이 진정인에게 불리한 경우, 진정인은 법원에 항소할 권리가 없다. 그러나, 진정인은 감독관의 결정에 대해 사법적 심사를 요청할 수 있으며, 이로 인해 일반적으로 모든 법적 문제에 대한 심사가 가능하지만 사건의 시비곡직에 관한 전반적인 재검토는 이루어지지 않는다. 지금까지 사법적 심사가 이루어진 진정건은 보고된 바 없으며, 단지 몇 건의 신청이 있었으나 불충분하여 법원에 의해 기각되었다.

결정이 정보 관리자에게 불리한 경우, 정보 관리자는 그 결정의 이행을 거부할 수 있으며 이로써 해당 진정인이 법원 심리를 요청하게 되면서 처음부터 다시 심리가 이루어지기 때문에 정보 관리자는 사실상 법원 항소권이 있는 셈이다. 감독관의 결정이 법원에서 강행된 적은 없다.

진정인과 정보 관리자는 모두 결정문에서 정한 보상금액의 검토를 요청하는 항소를 행정심판소(Administrative Appeals Tribunal)에 제기할 수 있다. 감독관이 결정문에서 보상금액을 정한 경우는 단 한 번이며, 해당 진정인은 낮은 금액에 이의를 제기하는 항소를 제기하였으며 승소하였다.

*1988년 사생활보호법*에 따라서 개인은 정보보호 원칙의 위반 또는 위반 위협에 대해 법원의 가처분명령을 요청할 수 있지만, 위반에 대한 구제를 직접 법원에 요청할 수는 없다. 감독관은 법원에 가처분명령을 신청할 수 있지만 지금까지 그러한 사례는 없다. 가처분신청 권한은 지금까지 단 한 번 사용된 적이 있는데, 두 상업적 기관의 분쟁건에 서였다. 실제로, 진정인은 법원이 아니라 감독관에게 진정을 제출하는데, 그 부분적인 이유는 상대방의 소송 비용을 자신이 부담해야 할 가능성이 있기 때문이다.

노던 테리토리 - 유사한 비활용 사례

정보감독관은 연방 감독관과 유사한 조사권을 지니며, 진정건에 대한 심리를 개최하기 전에 조정을 시도하여야 한다 (s.111). 조정이 성공하지 못하여 (Part 7, Division 2의 절차에 의거하여) 심리를 개최하면, 감독관은 연방 감독관이 내릴 수 있는 명령(최고 A$60,000의 보상 명령을 포함하여)과 유사한 명령을 한 가지 이상 내릴 수 있다 (s. 115). 당사자는 누구라도 감독관의 결정에 대해 대법원에 항소할 수 있지만, 법적 문제에 관하여만 가능하다 (s. 129). '어떠한 사유'로든 항소할 수 있는 권리('all grounds' right of appeal)가 없다는 것이 연방법의 경우에서와 마찬가지로 결점이라 할 수 있다. 또한, 감독관은 진정과 무관하게 사생활보호 감사(privacy audit)을 실시할 수 있는 권한이 있다 (s86(1)(e)). 노던 테리토리 감독관이 권한을 행사한 사례는 없다.

타스마니아 - 또 다른 부적절한 모형

어떠한 독립 법원이나 심판소에 대한 접근도 허용하지 않는 법이라는 측면에서 타스마니아 법은 어떠한 집행력 있는 구제방안도 마련되어 있지 않은 법이다. 옴부즈맨은 충분한 조사권을 지니고 있지만, 타스마니아 법의 사생활보호 원칙(PIPP)의 위반으로 판정한 후에 자문과 권고만을 할 수 있다 (s. 22). 권고는 접수된 날로부터 근무일 기준으로 5일 내에 의회에 상정하여야 한다 (s. 22(3)). 이러한 제도는 기관들이 부정적인 대외 이미지를 꺼려 자체적으로 진정을 해결하도록 어느 정도의 압력을 가하는 효과가 있다. 법에서는 정보 주체에게 PIPP 이행을 강제하는 결정을 확보할 수 있는 수단을 부여하고 있지 않다. 법원이나 행정결정심판소를 통해 PIPP의 시행을 꾀할 수 있는 통로도 없다. 미약한 "이름을 밝혀 창피주기(name and shame)" 조항 자체만으로는 EU 지침이나 기타 국제기준(APEC 기본틀은 제외하고)의 적정성 요건을 충족시키지 못한다. 타스마니아 감독기구 웹사이트에는 이 법이 활용된 적이 있음을 보여주는 자료가 없다.

8.4. 호주 주단위 – 대안적 모형과 독립적 심판소

호주의 두 주인 빅토리아와 뉴사우스웨일즈는 공공부문 사생활보호와 관련하여 보다 효과적인 집행체제의 특징을 보여주고 있으며, 또 다른 주인 퀸즈랜드는 최근에야 이와 유사한 모형을 채택하였다.

빅토리아

빅토리아의 감독관은 호주 연방과 뉴사우스웨일즈의 경우와 유사한 다양한 기능을 지니고 있다 (s.58). "개인 사생활(personal privacy)"에 관련된 권한은 "개인정보 사생활(privacy of personal information)"을 의미하지만 (s.3 (정의)), 공개 성명을 발표할 수 있는 권한을 포함한 감독관의 권한 중 상당수는 "개인의 사생활(the privacy of an individual)" 또는 "개인이 속한 계층의 사생활(the privacy of any class of individual)"을 가리키며 이는 신체적인 침해와 같이 정보 외(non-informational) 사생활의 측면을 포괄할 정도로 광범위한 의미를 지닌다.

감독관은 알선의 성공 가능성이 충분하다고 판단하면 진정건에 대한 알선을 시도해야 한다 (s.33). 알선 후에 당사자들이 합의에 도달하면, 당사자 일방은 그러한 합의가 있은 지 30일 내에 당사자 모두가 서명하고 감독관이 검증한 서면 합의를 작성하도록 요구할 수 있다 (s.33). 이 합의서는 VCAT에 등록할 수 있고, 등록과 함께 VCAT의 명령이 되어 그 내용들을 명령으로서 집행할 수 있다 (s.33(5)). 진정에 대한 알선이 성공할 가능성이 낮다고 감독관이 결정하면, 해당 진정인은 진정을 VCAT에 제출하도록 요구할 수 있다 (s.32).

VCAT는 진정에 대한 심리를 마친 후에 다음과 같은 명령을 포함한 광범위한 명령을 내릴 수 있는 권한이 있다.

- 진정의 대상인 행동의 지속을 금하는 명령
- 명령의 대상인 당사자가 손실 또는 손상(감정적 상처와 모욕을 포함)을 시정하기 위해 합당한 조치를 취하여야 한다는 명령
- 손실 또는 손상(감정적 상처와 모욕 포함)에 대해 $100,000를 초과하지 않는 보상금 지급 명령
- 해당 진정과 관련하여 진정인에게 합당한 비용을 변상하라는 명령
- 개인정보 수정 또는 해설 첨부 명령

이러한 권한은 연방의 1988 사생활보호법, 뉴사우스웨일즈의 1998년 사생활과 개인정보보호법에 명시된 권한과 상당히 유사하며, 단 보상금 최고액이 뉴사우즈웨일즈는 AUD40,000, 연방에서는 제한이 없다는 점에서 차이가 있다.

VCAT의 심리와 그에 따른 구제 조치는, 우선 행동규범 관리자(code administrator)에게 진정을 제출하였든지 (그 다음으로 감독관과 VCAT에 차례대로 제출), 적용되는 행동규정이 없어서 최초 진정을 감독관에게 제출하고 알선이 실패하여 그 다음으로 VCAT에 제출하였든지, 아니면 감독관이나 장관이 해당 진정을 직접 VCAT에 제출하였든지와 상관없이 궁극적으로 모든 진정인이 활용 가능하다. 이는 법의 한 강점을 보여주는 것으

로, 종국에는 모든 진정인이 동일한 구제, 동일한 독립적, 준사법적 항소기구에 접근할 수 있게 된다. 당사자 일방은 VCAT의 결정에 대해 빅토리아 대법원에 항소할 수 있다. 그러나, 정보보호원칙의 위반에 대한 진정을 VCAT나 법원에 직접 제기할 수는 없다.

또한, VCAT는 진정인 또는 감독관의 신청이 있는 경우, VCAT가 이후에 실시하거나 내릴 가능성이 있는 알선 또는 명령을 침해하는 조치를 당사자가 취하지 못하도록 잠정명령(interim order)을 내릴 수 있다 (s. 38).

진정의 대상이 된 행위를 지속하지 못하도록 VCAT가 s. 43에 의해 내린 명령을 어떤 조직이 이행하지 않은 경우, 이는 VCAT에 대한 모독으로 간주된다. 감독관이 어떤 조직이 IPP(또는 행동규범)를 위반하였다고 판단하고 그 위반이 "심각하거나 극악한 위반"(이에 대해서는 더 상세하게 해석하고 있지 않음)이거나 그렇게 심각하지는 않지만 상습적인 경우("지난 2년 내에 5회 이상"으로 정의)에는 형사상 처벌이 가능하다 (s. 44). 감독관은 자발적으로 또는 진정인의 신청에 따라(s. 44(5)), 해당 조직에게 향후 이행을 위한 구체적인 조치를 취하도록 요구하는 "이행 통지(compliance notice)"를 발부할 수 있다 (s. 44(2)). 그러한 경우에, 감독관은 폭넓은 조사권을 지닌다 (ss. 36-38). 한 조직이 이행통지를 이행하지 않는 것은 기소가능한 위법 행위로(s. 48), 감독관의 결정을 VCAT가 심사하도록 요청할 권리가 있다. 이 외에는, 법을 위반한다고 해서 형사상 책임이 발생하지는 않는다 (s. 7(2)).

뉴사우스웨일즈

'1998년 사생활보호와 개인정보보호법(PPIPA)'는 뉴사우스웨일즈 사생활보호감독관실("Privacy NSW")의 설립 근거가 되는 법이다. 이 법에는 11가지의 정보보보원칙(IPP)이 포함되어 있으며, 그 내용은 1988년 연방 사생활보호법의 원칙과 유사하다. IPP는 뉴사우스웨일즈 지방정부와 정보 서비스를 아웃소싱하는 정해진 기관들을 포함한 공공부문에 적용되며, 민간부문은 제외된다. 국유기업은 IPP의 적용 대상에서 제외되었다. 그 밖에도, 부규정(Ministerial regulation)으로 수립되지만 의회에서는 승인되지 않을 수도 있는 행동규약에 의한 경우를 포함하여, 여러 예외가 존재한다. IPP의 적용 방식을 수정할 수

있으며 그 적용 예외를 정할 수 있다.

공공부문 기관이 자신의 사생활을 침해하였다고 판단하는 사람이 구제를 받을 수 있는 통로는 두 가지가 있다. 먼저, PPIPA법 Part 4, Division 3에 의해 사생활보호감독관에게 진정을 제출할 수 있다. 이러한 진정은 "[개인의] 사생활 침해 또는 개입" 주장을 내용으로 할 수 있다. 이 용어들에 대해서는 정의하고 있지 않으며, 정보보호진정보다는 포괄적이며, 심지어는 민간부문에 대한 진정도 포함될 수 있다. IPP, 행동규범 또는 Part 6의 공개 등기부원칙(public register principles)을 위반한 경우는 감독관이 조사할 수 있는 사안에 포함된다 (s. 45(2)). 감독관은 알선을 통해 진정의 해결을 시도하여야 하며(s. 49), 조사가 완료되면 이를 바탕으로 보고와 권고만을 할 수 있다 (s. 50). 감독관은 진정건을 직접 ADT에 회부할 수 없으며 (이는 빅토리아의 경우와는 대조된다), 먼저 해당 기관에 의한 내부 검토를 요청해야 한다. 개인이 Part 4에 의해 사생활감독관에게 진정을 제출하기로 하고 감독관이 조사를 실시하는 경우라 하더라도, 이로 인해 그 개인이 Part 5에 의한 구제를 신청하지 못하는 것은 아니다.

두 번째 방법은 해당 개인이 IPP, 행동규범 또는 Part 6의 공개등기부원칙의 위반에 대해 해당 기관에 진정을 제출하는 것으로(s. 52), 해당 기관은 진정이 제출되면 내부 검토를 실시해야 한다 (s. 53). 해당 기관은 감독관에게 통보해야 하며, 감독관에게 기관을 대신하여 (수수료를 받고) 내부 검토를 실시해 주도록 요청할 수 있다 (s. 54). 진정인이 내부 검토 결과나 해당 기관이 그 결과 취한 조치에 만족하지 못하면, 내부 검토의 대상이 되었던 행위를 심사해 줄 것을 ADT에 요청할 수 있다 (s. 55(1)). 심판소 내에서는 단독위원의 결정에 대해 항소심판단(Appeal Panel)에 항소할 수 있는 권한이 있다. 이후에 뉴사우스웨일즈 항소법원에 항소할 수 있다.

심판소는 다음과 같은 명령을 내릴 수 있다 (s. 55(2)).

"(a) subsection (4)와 (4A)를 벗어나지 않는 범위 내에서, 해당 공공부문 기관에게 문제의 행위로 인해 발생한 손실 또는 손해에 대한 보상으로 신청인에게

$40,000를 초과하지 않는 손해배상금을 지급할 것을 요구하는 명령
(b) 해당 공공부문 기관에게 정보보호원칙 또는 사생활보호 행동규범을 위반하는 행위 또는 조치를 삼가도록 요구하는 명령
(c) 정보보호원칙 또는 사생활보호 행동규범의 이행을 요구하는 명령
(d) 해당 공공부문 기관에게 공개된 개인정보를 수정하도록 요구하는 명령
(e) 해당 공공부문 기관에게 신청인이 겪은 손실 또는 손해를 구제하기 위한 구체적 조치를 취하도록 요구하는 명령
(f) 해당 공공부문 기관에게 공개 등기부에 포함된 개인정보를 공개하지 말도록 요구하는 명령
(g) 심판소가 적절하다고 판단하는 부수적 명령"

심판소는 "신청인이 해당 공공부문 기관의 행위로 인해 금전적 손실이나 정신적 또는 신체적 상해를 입었다"고 확신하는 경우에 한하여 금전적 보상 명령을 내릴 수 있다 (s. 55(4)).

심판소에 접수된 모든 검토 요청은 감독관에게 통보되어야 하며(s. 55(6)), 감독관은 검토 과정에 참석할 권리가 있다 (s. 55(7)).

NSW 사생활보호법과 관련하여 NSW ADT가 심리한 진정건은 약 150건에 이르지만, 다수의 경우가 매우 기술적인 문제에 관한 것이며, 정보보호원칙의 해석이나 구제 제공에 관한 실질적인 문제와 관련된 경우는 상대적으로 적다[12]. 두 건의 경우에만 NSW 대법원 항소 절차를 밟았다.

7건의 ADT 결정문은 s. 55에 의한 보상 문제를 논하고 있다. 심판소는 대체로 보수적인 입장을 취하고 있다. 피고의 법위반에 의해 손실이 발생하였음을 입증한다고 해서 자동적으로 손해배상이 이루어지는 것은 아니다 (그 예로, *NW vs. NSW 소방대 사건*(No.2) [2006] NSWADT 61 참조). 우울증과 불안에 대해서는 A$5,000의 보상금 지급 결정이 내려졌으며(*WT vs. Auburn Council* [2007 NSWADT 253), 진정인의 정신 상태에 대한 오진을 포함하는 보고서를 잘못 공개한 경우에 대해서는 A$7,500의 보상금이 결정되었다

12) 호주의 사생활보호 관련 사례는, <http://www.austill.edu.au/au/other/AUPrivCS/>에서 '호주 사생활보호 사례 요약집(Australian Privacy Case Summaries)' 참조.

(*JD vs. NSW Medical Board* (No.2) [2006] NSWADT 345). 또한, 진정인의 정보를 잘못된 주소에 보낸 기관으로 인해 야기된 고충에 대해서는 A$2,000의 보상금 지급이 결정되었다 (*RD v. Department of Education and Training* [2005] NSWADT 195).

따라서, NSW 법의 집행체제로 인해 이 법에 대한 상당히 많은 양의 해석이 축적되었으며, 법규정의 의미는 심판소에 의해 점차 명확해지고 있다. ADT 제소 사건 중에도 많은 금액은 아니지만 진정인에게 보상금이 지급된 사례가 보고되고 있다. 이러한 사례가 타 정보처리기관들에게 내부 검토가 지시된 진정건의 해결을 위해 보상금을 지급하도록 유도하였는지는 알려져 있지 않다.

퀸즈랜드

퀸즈랜드의 신설법에 의해 개인은 기관에 의한 자신의 개인정보 취급에 관하여 먼저 해당 기관에게 내부 검토를 요청하는 진정을 할 수 있고 (s. 166(2)), 그 기관이 진정을 해결하지 못하면 그 다음으로 감독관에게 진정할 수 있으며, 감독관은 해당 진정을 조정하기 위한 모든 합당한 조치를 취하여야 한다 (s. 171). 성공적인 조정 합의서의 내용은 감독관의 인증을 받은 후에 QCAT에 의해 시행된다 (s. 172와 s. 173).

이 법은 서면상으로는 기한 요건에 있어 너무 엄격하고, 감독관에게는 진정인의 '협조 부족' 또는 기타 이유로 진정건 조사를 중단할 수 있는 자유를 지나치게 많이 부여하고 있다 (s. 168). 진정인은 (뉴사우스웨일즈의 경우와는 대조적으로) 감독관을 거치지 않고 내부 검토 후 바로 심판소나 법원에 진정을 제출할 수 없다 (s. 39). 법이 호의적으로 운영되느냐 여부에 따라 크게 좌우될 것으로 보인다.

조정이 성공하지 못하면, 진정인의 요청이 있는 경우에 한하여 해당 진정이 감독관에 의해 QCAT에 회부된다 (s. 176). 심리를 마치면, QCAT는 사생활보호 원칙의 위반에 대해 지속적 위반 행위 금지, 사과, 최고 A$100,000의 보상금, 진정에 소요된 비용 변상 등의 다양한 구제조치를 지시하는 명령을 내릴 수 있다. 이러한 방식은 빅토리아의 법률에서 채택하고 있는 방식과 매우 유사하다.

IPP 위반 행위에 대해 감독관은 기관에 이행 통지를 발부할 수도 있으며, 단 그 위반 행위가 '심각 또는 극악하거나' 지난 2년 간 5회 이상 발생한 경우에 한한다 (s. 158). 해당 기관은 이행을 위해 모든 합당한 조치를 취하여야 하며, 그렇지 않은 경우에는 민사상 처벌을 받을 수 있다 (s. 160). 기관은 QCAT의 검토를 요청할 수 있다 (s. 161).

이 외에도, 감독관은 어떠한 체계적인 사생활보호 이슈에 대해서도 검토를 실시하고, 의회에 검토 결과를 보고하며, 법에 의한 어떠한 개체에 대해서도 '이행 감사를 실시'하고, 공공부문과 관련된 어떠한 사생활보호 이슈에 대해서도 의견을 개진하며, 법의 적용과 '사생활보호와 관려된 일반적 모범 관행'에 대해 가이드라인을 발표하는 등의 폭넓은 권한을 지닌다 (s. 137). 이러한 임무를 수행할 수 있는 감독관의 예산 규모에 따라 많은 부분이 좌우될 것으로 보인다. 예산은 정부가 결정하지만, 그 외에 선결과제 선정이나 권한 행사에 있어 감독관은 지시를 받지 않는다 (s. 134).

또한, 감독관은 IPP를 이행해야 할 기관의 의무 면제 또는 수정을 승인할 수 있는 권한이 있다 (s. 157). 이러한 적용 예외는 연방법에서는 '공익 결정(Public Interest Determinations)'라고 부르며, 이 법에서와 마찬가지로 감독관은 의무의 면제 또는 수정이 공익을 위한 것이라고 확신하여야 한다. 퀸즈랜드 법에는 그러한 승인이 이루어지기 전에 공청회나 의견 개진(submission)이 있어야 한다는 조항이 없지만, 승인은 하위 법률로 취급되며(s. 157(2)) 따라서 의회에 의해 기각될 수 있다.

8.5. 뉴질랜드 – 발전된 형태의 심판소 제도

뉴질랜드의 *1993년 사생활보호법*의 집행은 사생활보호감독관에게 접수된 진정 또는 감독관의 '자체 발의' 조사에 의해 추진된다. 감독관은 두 가지 모두와 관련하여 상당한 조사권을 지닌다. 현재 감독관이 다루는 진정건은 연간 650건으로, 대부분은 접수된 해에 종료된다. 상당수의 진정이 합의로 해결되며, 감독관은 일단 합당한 해결책이 제시되었다고 판단하면 더 이상 관여하지 않는다. 감독관은 구속력 있는 명령을 내릴 권한은 없지만 (민간부문에서의 접근 혐의(access charges)와 관련된 경우는 제외하고), 적절한

사안의 경우에는 (가령, 당사자들이 합의에 도달할 수 없는 경우) 인권소송담당관(Director of Human Rights Proceedings)에게 회부하여 인권심판소(HRRT)에서의 민사소송이 개시되어야 하는지 여부를 결정하게 할 수 있다. 2005년 이후로, 감독관이 심판소로 이관시킨 진정건은 매년 최고 20건에 달한다. 진정인도 감독관의 조사가 끝난 후 (가령, 감독관의 결정이 불만스러우면) 진정을 인권소송담당관에게 제출하거나, 감독관의 조사 여부와 관계 없이 직접 심판소에 제출할 수 있다. 매년 약 20건의 사생활보호 관련 진정건이 HRRT에 접수되고 있다.

인권심판소는 선고(declaration)를 내리고(가장 일반적인 구제책), 지속되는 위반 행위를 금하는 명령을 하고(그다지 엄격한 금지 명령은 아님), 감정적 상처를 포함한 피해보상을 명할 수 있는 권한이 있다. 현재까지 책정된 가장 높은 보상금액은$40,000이며, 그 다음은 NZ$20,000이다. 잘못 수집된 정보, 보안 장치 미비, 잘못된 접근 거부, 데이터베이스에 부정확한 정보 보유, 부당한 정보 공개 등에 대해 손해배상이 인정된 경우가 상당수에 이른다 (상세한 내용은 Roth 1993-2009 참조).

HRRT의 판정에 대해 고등법원에 항소할 수 있으며, 법적인 문제에 한해서는 항소법원에 추가로 항소할 수 있는 권리가 있다 (이를 위해서는 고등법원이 항소 허가(leave to appeal)를 하거나 항소법원이 특별 항소 허가(special leave to appeal)를 해야 한다). 지금까지 사생활보호와 관련하여 고등법원이 심리한 항소건은 23건이었으며, 항소법원이 심리한 항소건은 1건이다. 사생활보호 문제와 관련하여 HRRT가 내린 결정은 161건이며, 주로 법적 논거를 내용으로 하고 장황한 경우도 적지 않다. 사생활보호 감독관도 IPP가 특정한 상황에서 어떻게 적용되는지에 관한 감독관의 의견을 담은 258건의 사건 비망록(case notes)을 발표하였다. 이러한 사법적, 준사법적 결정과 감독관의 행정해석으로 인해, 뉴질랜드는 아시아-태평양 지역에서 단연코 가장 방대한 사생활보호법(경성법과 연성법 포함)을 갖춘 나라다. 뉴질랜드법은 가장 충실하게 '해석되어' 있으며, 이러한 충분한 해석으로 이득을 본다고 할 수 있는 유일한 국가일 것이다.

8.6. 한국

[여기에서는 다루지 않고 이후 출간되는 책자에서 다룰 예정임]

8.7. 일본 – 책임의 부재?

일본에는 중앙 정보보호기구가 설립되어 있지 않아서 사생활법 분할되어 집행될 수 밖에 없다. 또한, 이 법이 이러한 분산화된 구조를 통해 얼마나 효과적으로 집행되고 있는지에 대한 정보도 부족한 것으로 보인다.

민간부문

PPI법에 따라 기업의 개인정보처리에 대한 진정은 4개 기구 중 한 곳에 제출할 수 있다.

(ⅰ) *해당 기업체* - 기업 운영자는 '해당 진정을 적절하고 신속하게 처리'하기 위해 '노력하여야 한다' (A 31)

(ⅱ) *인가된 개인정보보호기관(APIPO)* - A 37에 의해 소관 부처 장관이 지정한 34개 기관이 있으며 (2007년 5월 31일 현재)이에 대해서는 자율규제와 관련하여 뒤에서 논하도록 한다.

(ⅲ) *지방정부부처* - 지방정부의 장은 진정 처리와 관련하여 소관 부처의 장관과 동일한 권한을 지닌다 ('행정명령'에 관한 내용 참조).

(ⅳ) *일본의 중앙소비자사무협의회(NCACJ)* - 지방의 소비자센터를 통해서도 가능하다. 기본정책(일본, 2006)에 의해 NCACJ는 자문 제공, 훈련 실시, 자료 배포, 소비자 센터와 같은 '고충처리기관' 지원 등의 책무를 수행한다.

PPI법에는 개인이 APIPO, 지방정부부서, NCACJ 또는 '소관 부처 장관'에게 진정을 제출하도록 허용하거나 진정은 우선적으로 해당 기업체에 제출하여야 한다는 구체적인 규정이 없다.

NCACJ는 '개인정보처리신고 매뉴얼(Manual on Complaint Processing for Personal

Information'과 '개인정보보호 관련 신고 및 대응 개요(Summary of Personal Information Protection-related Complaints and Responses)'를 제작하여 배포한다. 영어판은 제작하지 않는다. NCACJ와 내각부(Cabinet Office)는 신고 사례를 수집하여, 2006년부터 자료를 교류하고 있다 (일본, '삶의질정책위원회(Quality of Life Policy Council), 2007:29).

2005년 회계연도에는, 14,028건의 신고가 지방정부나 NCACJ에 접수되었다 (일본, 삶의질정책위원회, 2007:2). 개인정보보호 인가기관에 접수된 건수는 언급되지 않고 있다.

2007년 회계연도에는, 지방정부와 NCACJ에 접수된 신고건이 12,728건이었으며, 그 중 85%는 지방 소비자센터에 접수되었다. 신고의 주된 내용은 개인정보의 사기성 확보, 정보의 유출이나 소실, 이용 목적 외 공개가 주를 이루었다 (내각부, 2008). 안타깝게도, 이러한 내용의 신고건수를 모두 더해보면 17,000건이 넘기 때문에, 퍼센트 수치는 신뢰할 수 없을 것 같다. 12,728건의 신고에 대한 대응 결과는 12,094건(95%)이 '지도와 자문' 또는 '기타 형태의 정보제공'이었으며, 212건(1.7%)은 성공적으로 조정되었고, 나머지 대부분은 타 기관으로 이관되었다.

이러한 신고건이 행정부처에서 조사되는 진정으로 이어지는 것으로 보이지는 않는다. 따라서, 이와 같이 수 많은 신고건으로 인해 강제적인 제재가 부과되는지도 분명치 않다.

NCACJ 웹사이트[13]는 2004-2007년 신고건 중 18건에 대한 요약본을 게시하고 있지만, 그 이후로는 해당 자료가 없다. 따라서, 법위반이 어떤 결과로 이어지는가를 기업이나 일반인에게 보여주는 '피드백'이 거의 없는 실정이다. 따라서, '대응적 규제' 체제의 핵심 요소가 결여되어 있는 듯하다.

민간부문 - 행정명령

PPI법에 따라, 소관부처 장관(후술 내용 참조)은 기업 운영자에게 개인정보처리에 관

13) NCACJ website <http://www.kokusen.go.jp/jirei/j-top_kojinjoho.html>

한 “보고서를 작성”하게 “할 수 있으며”(A 32), 장관은 해당 기업 운영자에게 “자문을 제공”할 수 있다 (A 33). 이 보고서가 특정 신고에 관한 것인지 여부나, 개인이 어떠한 방식으로 신고하는지에 대해서는 명확하지 않다.

기업이 정보보호조항(A 16-27, 단, A 19와 A 30(2)는 제외)을 위반한 경우, 소관부처 장관은 해당 기업에게 “해당 위반 행위를 중단하고 이를 시정하기 위한 기타 필요한 조치를 취하도록” 권고할 수 있다 (A 34(1)). 기업이 권고를 이행하지 않고 장관이 ‘개인의 권리와 이익이 심각하게 침해될 수 있다’고 판단하면, 장관은 기업에게 권고된 조치를 취하도록 명령할 수 있다(A 34(2)). 특정한 상황에서는 권고를 거치지 않고 장관이 긴급명령을 내릴 수 있다 (A 34(3)). 요컨대, 통상적인 경우에는 기업 보고서 요청, 권고, 명령의 세 단계를 거친다.

‘소관부처 장관’은 ‘해당 기업 운영자의 부문에 대해 관할권을 지닌 해당 장관 등’을 가리키며 (A 36), 단, 고용관리와 관련된 개인정보의 경우에는 보건노동복지부장관도 책임이 있다. 총리가 소관부처 장관을 지정할 수도 있다.

2007년 회계연도에는, 장관이 관할권내 기업들로부터 보고서를 받은 경우가 83건이지만, 권고를 하거나 명령을 내린 경우는 없다. 2006년에는, 60건의 보고서 제출에 대해서 4차례의 권고가 이루어졌다 (내각부, 2008). Ito와 Parker(2008)는 지금까지 일본에서 법에 의한 집행절차가 진행된 경우는 매우 제한되어 있다고 지적한다.

> 현재까지 진행된 주요 집행절차의 하나는 2005년 지역 은행에 대해 제기된 사건이었으며, 이 사건은 은행이 약 130만명의 고객에 관한 개인정보가 담겨있는 세 개의 CD-ROM을 분실한 것이 발단이었다.[14] 이 사건은 지역 재정국의 엄중한 지탄으로 이어졌으며, 해당 은행 담당자들에게 경고가 주어졌다. FSA는 단연코 가장 활성화된 정부부처다. 2007년과 2008년 3월 사이에 개인정보처리기관으로부터 제출 받은 83건의 보고서 중에서, 78건이 FSA의 명령에 의한 것이었다 (대부분이 정보보안조치와 유출방지조치 관련). 그러나, 이 기간 중에 개선권고가 내려진 경우

14) “Michinoku ordered to secure data” (The Japan Times, May 23, 2005).

는 없었다.

단순히 보고서 제출을 요청하면 적절한 경우에 항상 구제제공으로 이어진다는 확실한 증거가 있지 않는 한, 일본에서 장관의 감독이 대응적 규제 체제에서 중요한 역할을 하고 있는 것으로는 보이지 않는다. Ito와 Parker(2008)는 이 법이 경고의 효과는 어느 정도 있을 수 있다고 보았다.

> 유럽의 경우와 같이, 이 법의 실질적인 효과는 기업이 대외 이미지에 손상을 입을 수 있다는 위기감을 조성하는 것이다. 실제로, 시행 조치가 미흡한 것은 부분적으로 일본사회의 성격에서 그 원인을 찾을 수 있다. 일본은 복잡한 상도덕 체계를 갖고 있으며 기업 이미지는 여전히 상당한 중요성을 띤다. 개인이나 기업모두에게 (정도는 약하지만, 외국 기업체도 포함) 평판은 상당히 중요한 것으로 인식되고 있으며 행정규칙의 엄격한 이행에 대해서도 마찬가지다. 일본 기업들은, 다른 이행문제들과 같이 정보이행문제에 대해서도 다른 국가보다 더 진지하게 다루어지고 있으며 비공식적인 법집행 위협만으로도 미이행 기업을 움직이는 데 충분하다고 주장하곤 한다. 2005년 지역은행에 대해 취해진 은행장 지역 재정국 소환 등의 집행절차의 성격과 은행 담당자들에 대한 경고 조치는, 적어도 행정 당국의 입장에서는 기업 임원들을 통해 기업에게 겁을 줌으로써 법이행을 확보하려는 의지가 있음을 보여준다.
>
> 그러나, 일본 기업들이 다른 국가의 기업에 비해 정보보호이행 성적이 더 좋다는 주장을 뒷받침할 증거는 많지 않다. 실제로, 기업들이 법 위반과 관련하여 신문의 1면을 줄줄이 장식하고 있는 현 상황은 일본에서 정보보호이행 문제가 다른 경제대국의 경우와 마찬가지로 만연해 있는 문제라는 주장을 뒷받침할 수 있는 실례다.

형사처벌

정보사생활보호 원칙의 위반은 그 자체만으로는 어떠한 법에 의해서도 형사처벌의 대상이 되지 않는다. PPI법에 의하면, 장관의 명령을 위반하여야 형사처벌이 주어진다. A 34에 의한 장관명령을 위반하게 되면 최고 ¥30,000 (US$3,000)의 과징금(과 해당 정보관리자가 개인이면 최고 6개월의 징역행)이 부과된다 (A 56~57).

공공부문 법규에는 형사처벌에 대한 일반 규정이 없지만, 직원 또는 이전 직원이 부당하게 개인정보를 공개하거나 수집하는 경우, 특정 상황에서는 형사처벌이 주어질 수 있으며(PPIHAO법 A 53~55) 일본 외에서의 범법행위에 대해서도 마찬가지다. 이 법은 그러한 정보의 수혜자에 의한 범법행위에 대해서는 기술하고 있지 않다.

민간분쟁해결기구

'개인정보보호 인가기관(APIPO)'의 역할은 Part 4, Section 2(민간기관의 개인정보보호 증진)에 명시되어 있다. '기본정책(Basic Policy)'에 따르면, APIPO는, 특히, 기업들이 자발적으로 민원을 해결하도록 지원함으로써, 일본의 정보보호에 있어 '지극히 중요한 역할'을 수행하게 될 것으로 기대하고 있다.

소관부처 장관은 해당 부문에서 타 기업('대상기업(target)'으로 칭함)의 개인정보처리 관행에 관한 신고 처리에 관여하고 있는 기업을 APIPO로 인가할 수 있다. (A37). APIPO 인가 신청기업이 충족해야 하는 기준은 매우 모호하다(A 39). 그 외 모든 기업(대상기업)은 분쟁해결기구의 회원으로 가입하여야 하며 이를 공표하여야 한다(A 41). APIPO는 개인으로부터 직접 신고를 받을 수 있으며, 대상기업들은 조사에 협조할 의무가 있고 APIPO의 요청에 대해 '타당한 근거가 없이는' 거부할 수 없다(A 42). 각 APIPO는 자체 가이드라인을 공표하도록 되어 있다(A 43). 장관은 APIPO에게 보고서 제출을 요구하거나(A 46), 절차 개선을 명하거나(A 47), 인가를 취소할 수도 있다 (A 48). 2007년의 경우, 장관이 보고서 제출을 요구한 경우는 한 차례 있었다 (내각부, 2008:4).

APIPO는 독자적인 권한이 전혀 없다. 분쟁의 중재자도 아니며 조정자 권한을 부여 받는 것도 아니다. 회원 기업들과 진정인 사이에서 중립을 취해야 하는 것처럼 보이지만, 이것도 분명하지는 않다.

A 37에 의해 해당 장관이 지정한 APIPO는 (2007년 5월 31일 현재) 34곳에 이르지만, 2005년에 APIPO에 접수된 신고건수는 삶의질정책위원회가 공개한 바 없다. 이 위원회는 이러한 민간분쟁해결기구의 중요성을 강조한 '기본정책'의 내용을 지지하고 있지만,

적어도 일부 APIPO에 대해서는 간략한 비판의 내용을 발표하기도 하는 것으로 보인다. 위원회는 '적극적이지 못한 인가기관들은 향후에 적극적으로 신고를 처리하고 대상기업들에게 정보를 제공할 것으로 기대한다'고 지적하고, 다음과 같이 덧붙였다.

> 앞으로는 개인정보보호 인가기관의 역할을 일반인과 기업들에게 충분히 알리고 이 기관들에 대한 신뢰를 개선하기 위한 노력을 기울이는 것이 중요하다. 또한, 이 기관들이 자체 기능을 더욱 향상시키기 위해 개인정보유출사건에 적극적으로 관여하여야 할 것이다.

이 기관들의 실효성에 대해 위원회가 제시한 자료는 없다. 그러한 자료가 없는 상태에서, APIPO가 효과적으로 운영되고 있다고 결론짓는 것은 타당하지 않다.

공공부문

일본 공공부문에서는 구제를 확보하기가 훨씬 더 어렵다. 개인의 기록에 대한 접근, 수정 또는 사용 중단과 관련하여 행정기관이 내리는 결정에 항소하는 경우, 그 항소를 판정하여야 하는 해당 행정기관의 장은 '정보공개 및 개인정보보호심사위원회'와 협의하여야 한다 (PPHIAO 법, 42조). 그러한 협의의 결과는, 접근 요청을 받은 개인정보 파일의 공개에 반대하였던 제3자를 포함하여 모든 관련 당사자들에게 알려야 한다.

8.8. 대만 – 실효성 없는 분산화된 집행체제의 또 다른 예

대만의 1995년 '전산처리개인정보보호법(Computer Processed Personal Data Protection Act)'에 의하면, 단독 감독기구는 없으며, 법집행은 각 산업부문의 소관부처에 일임되어 있다. 이 법의 이행이나 실효성에 대한 증거 자료는 부족하지만, 논평가들은 이 법이 실효성이 없다고 주장한다 (Peng(2003)은 이 법을 '미흡하고 결함이 많다'고 평하였고, Tang(2009)는 '많은 결점'을 지적하였으며, Chuang(2003)은 '허점 투성이'라고 표현하였다), 그 이유로는 모호한 규정(Peng(2003), Tang(2009)), 제한된 범주(Tang(2009)), 포괄적인 감독기구의 결여(Tang(2009))를 들고 있다. 정보이동제약에 관하여 매우 제한적으로 다루고 있는 현 조항들이 시행되고 있는지에 대해서는 알려진 바 없다.

개혁안

대만 행정부(Executive Yuan)는 2000년 이후로 이 법을 강화하기 위한 여러 대책을 제안하여 왔지만(Tang(2009)), 아직까지 중앙감독기구 설치 제안은 이루어진 바 없다. 2005년에 법안이 도입되었고, 법무부는 2007년에 법승인을 재요청하였다. 마잉주 대만 총통의 신정부는 2009년 1월에 입법부(Legistrative Yuan)에 법안을 제출하였으며, 현재 2차 검토가 개시되기 전에 정당간 교섭을 기다리고 있다 (Tang, 2009). 2008년 8월 대만에서 발생한 가장 큰 규모의 신분도용 사건이후로, 입법 압력이 높아졌다. 개혁안에는, 이 법의 적용범위 확대와 함께, 보상금과 행정처벌의 상한선을 높이고 등의 강력한 구제방안과 위반행위에 대한 집단 소송을 허용하는 내용이 포함되어 있다(Tang, 2009). 그러나, 중앙감독기구의 설립은 포함되어 있지 않다. 따라서 대만의 정보보호법은 그 실효성에 있어 아직까지는 매우 제한적이지만, 크게 향상될 가능성이 높다는 타당한 전망도 제시되고 있다.

9. 결론 – 대응적 규제를 위한 권한과 책무

일본과 대만의 정보보호법 이행을 위한 분산화된 방식이 효과적으로 실시되었다는 증거가 부족하다는 점을 감안하면, 이 국가들의 경험은 대부분 무시해도 좋을 듯하다. 소관부처가 정보보호법을 어떻게 집행하고 있는지는 전혀 투명하지 않으며, 이 때문에 그러한 집행 방식에 대한 완전한 이해는 불가능하다. 미국의 분산화된 집행 경험이 오히려 더 유용할 듯한데, 적어도 미국 연방공정거래위원회의 법이행 조치 일부는 효과적으로 평가되기 때문이다. 그러나, 이는 이 글의 주제에서 벗어나므로 다루지 않는다.

정보보호법 집행과 관련한 지역 경험에 비춰, 상대적으로 더 효과적인 것으로 판명된 방식에 관하여 어느 정도 임시적인 결론을 내릴 수 있다.

9.1. 진정 조사를 통한 집행의 실효성 확보

우선, 이 지역 DPA의 대부분 활동은 사후적 성격을 띠며, 접수된 진정건을 바탕으로 잠정적 위반 행위를 조사하는 권한에서 비롯한다. 이 활동에 DPA의 예산이 가장 많이 할당된다.

실효성 또는 실효성 부재와 상관관계에 있는 것으로 보이는 요소들은 무엇인가? 필자가 이 지역의 DPA 연혁을 관찰한 결과와 입수된 정보를 바탕으로 정리한 일차적 견해는 다음과 같다.

- DPA가 진정건에 대한 대응으로서 뿐만 아니라 자발적으로 (‘자체 발의’) 조사할 수 있어야 한다는 필요성 (호주 연방, 뉴질랜드, 홍콩)
- DPA가 자발적으로(‘자체 발의’) 잠정적 위반사건을 조사할 수 있는 권한은 그러한 조사가 진정과 동일한 지위를 갖고 동일한 집행 결과를 가져오는 경우에 더 효과적일 것이다 (호주 연방감독관의 경우와 대조).
- 집행력이 DPA에 주어지는 경우(호주 연방감독관)보다 독립적 심판소가 집행력 있는 결정을 내릴 가능성이 더 높다 (뉴질랜드 HRRT, NEW ADT, 정도는 약하지만 호주 빅토리아주의 VCAT).
- 직접적으로든(뉴질랜드), 기관의 내부 심사를 거친 다음이든(NSW), 아니면 DPA에 의한 조사 실시 후에든(빅토리아, 퀸즈랜드) 진정인에게 심판소의 심리를 허용하는 것이 필수적이며, 이러한 심리의 불허는 중대한 결함이 된다 (호주 연방감독관).
- 일반 법원을 통해서만 보상금 지급이 결정되는 것은 비효과적이다(홍콩).
- 심판소가 위반사실에 대해 보상금을 결정하도록 허용하더라도 상당한 액수를 정하는 오남용 사례는 없어서, 대체로 비교적 적은 금액이 결정되고 고액(US$ 20,000 초과)인 경우는 매우 드물다.
- 위반 행위가 반복될 가능성이 높은 경우에 한하여 범법행위로 제한한다는 것은 법 위반 행위 대부분에 대해 제재가 가해지는 경우가 거의 없음을 의미한다(홍콩).
- 법적 문제에 한정해서만이 아니라 ‘어떠한 사유로든 (on all grounds)’ (분쟁의 사실

관계 해석을 포함) 법원에 항소할 수 있는 권리는 필수적이며(뉴질랜드, 빅토리아, NSW), 이러한 권리가 결여된 곳에서는 법이 거의 발전하지 못하고 있다(호주 연방 감독관, 일본).

- 타당한 권리를 주장하는 진정인에게 법률 지원을 함으로써 실효성을 높일 수 있다(뉴질랜드).
- 정보보호체제의 효과적인 운영을 위해서는, DPA의 권한 활용, 진정인과 해당 기관에 대한 처리 결과(특히, 조정 해결건에 관하여)에 대한 DPA의 객관적이고 상세한 보고가 필수적이다. 그러한 보고가 없다면, (a) DPA의 실효성에 대해 어느 누구도 신뢰하지 않으며, (b) 진정인과 피진정인 모두가 규제 체제를 효과적이라고 여기고 그에 맞추어 (진정절차를 개시하거나, 불필요한 진정을 피하거나, 위반을 피하거나 위반행위를 시정하는 등) 행동을 수정할 수 있는 피드백을 받을 수 없다. 법집행과 구제 측면 모두에 있어 가장 세부적인 보고서는 심판소에서 작성되고 있지만(뉴질랜드 HRRT, NSWADT), DPA도 보고서를 통해 매우 세부적인 내용을 제공할 수 있다(뉴질랜드 감독관, 홍콩 감독관의 s. 48에 의한 보고서). 상대적으로 실효성이 떨어지는 체제의 경우에 보고 내용이 가장 상세하지 않았다(2003년 이후 NSW 감독관, 호주 연방감독관, 일본).

아직까지 효과적인 집행과 명확한 상관관계는 밝혀지지 않았지만, 일부 DPA에서는 다음과 같은 혁신적 특징들이 바람직한 것으로 보인다.

- 실제 진정진이 존재한다는 전제하에 진정인 집단을 대표하는 '대표 진정'을 인정한다(호주 연방, 뉴질랜드, 홍콩). 그러나 실제로는 호주에서 1건의 사례가 있었으며, 뉴질랜드는 그러한 사례가 전혀 없다.
- NGO가 개인 진정인을 대변할 수 있도록 허용한다(호주 연방). 뉴질랜드에서는 인권소송국장(Director of Human Rights Proceedings)에게 개인 집단을 대표하여 민사소송을 개시할 수 있는 권한이 있다(s82(4)).
- 정보보호원칙을 위반할 가능성이 있는 행위에 대한 진정건을 조사할 수 있는 권한과, 그러한 위반을 중단하게 하는 권한(호주 연방).

- 정보보호원칙의 위반 가능성 또는 위반을 방지하기 위해 법원의 금지 명령을 요청하는 DPA의 권한은 바람직한 것으로 보이지만, 그러한 권한이 존재하는 경우에도 거의 활용되지 않고 있다(호주 연방). 행위
- 분쟁해결을 지원하기 위해 독립적 조정을 알선할 수 있는 역량(뉴질랜드).

위반행위에 대해 (검찰에 고발하는 대신) 직접 사법조치할 수 있는 DPA의 권한은 홍콩 감독기구가 추진해오고 있으나, 홍콩정부는 불필요하다는 이유로 반대하고 있다(협의문서(Consultation Document), 2009:32).

장관이나 기타 기관의 요청 또는 지시에 의해 진정건을 조사할 수 있는 DPA의 권한은 이 지역의 DPA 업무에서 중요한 역할을 하고 있는 것으로는 보이지 않는다.

9.2. 기타 기능과 권한

진정건 조사와 관련이 없는 DPA 기능은 사전적 요소와 사후적 요소가 결합되어 있는 경향을 보인다.

규약 제정과 원칙 조정

이 지역의 정보보호법규는 거의 모두 특정 범주의 정보관리자나 개인 관리자에 대해 사생활보호원칙의 변경을 허용하는 부문별 '행동규약'의 제정이나 그와 유사한 방식의 채택을 허용하는 조항을 담고 있다. 이러한 조항은 국가에 따라 상당한 차이를 보인다. 호주 민간부문의 경우, 행동규약은 완전한 공동규제(co-regulation)가 가능하여, 사생활보호감독관에 대한 항소권을 제외하고 법의 모든 운용을 대신할 수 있다. 호주 연방과 NSW의 공공부문에서는, 감독관에게만 정보보호원칙 수정 권한이 주어져 있다. 홍콩에서는 행동규약은 이행하여야 한다는 가정을 전제로 하지만, 정보관리자가 법 이행을 입증할 수 있는 경우에는 규약 이행 의무는 반박할 수 있다. 이러한 차이들은 DPA의 권한뿐만 아니라 전체적인 규제체계의 구조에도 영향을 미친다.

행동규약을 제정하고 원칙을 변경하는 데 있어 DPA가 수행할 수 있는 역할에도 상당한 차이가 있다. 홍콩에서는 감독관이 자신이 또는 다른 사람이 제정한 규약을 공표할 수 있으며, 정보사용자나 그 밖의 적절하다고 판단하는 사람들과 협의하여야 한다(s 12). 호주 민간부문에서는, 민간부문 기관들이 감독관에게 규약 제정을 신청하여야 하며 (s18BA), 감독관은 규약을 제정하기 전에 여론 수렴의 기회를 제공하여야 한다(s18BB). 이 규약은 의회에 의해 기각되지 않는다. 여론 수렴은 호주 연방공공부문에 적용되는 원칙의 변경과 관련하여서도 요구된다. NSW의 공공부문에서는 감독관 또는 기관이 규약안을 제시할 수 있으며(s 31), 감독관은 협의를 거쳐야 하며 (충분한 협의를 거치지 않은 경우에는 비난 받을 수 있음), 장관은 s 31에 의해 제안된 규약을 제정하지만 그 내용을 변경할 수는 없다. 뉴질랜드 감독관은 주도적으로 또는 요청에 의해 법적 구속력을 지니는 행동규약을 공표할 수 있으며 (s 47), 공표하기 전에 의견 제출을 요청하여야 한다. 이 규약은 의회에서 기각할 수 있다.

그 형태가 어떻든 간에, 대부분의 관할권에서 행동규약 제정이나 정보보호원칙 수정이 이루어진 경우는 소수에 불과하다. 이러한 규약이 법에서 갖는 역할은 예상보다 약하다. 홍콩에서는 두 건의 규약만이 제정되었는데, 모두 특별한 사유 때문이었고(신분증과 신용정보), 호주에서도 소규모 부문에서 두 건만이 운용되고 있다 (퀸즈랜드 클럽과 시장·사회조사 부문). 지난 20년 동안 호주 연방공공부문에 적용되는 정보보호원칙이 수정된 경우는 10건에 불과하다. 뉴질랜드의 경우, 현재 운용되는 행동규약은 세 건뿐으로, 보건정보, 통신, 신용과 관련되어 있으며, 특정 고유 식별자와 관련하여 한 가지 원칙을 수정한 경우가 두 건 있었다.

NSW는 규약 승인과 원칙 수정 비율이 상대적으로 높다. 10년 동안 법 Part 3에 의해 제정된 행동규약은 11건이며, 조만간 9개가 추가로 제정될 예정이다. 이 규약은 법정 규칙이 아니기 때문에 의회의 기각 절차가 없지만 규약 제정 절차가 남용되고 있는 것으로는 보이지 않는다. s. 41의 지시(Directions)도 광범위하게 활용되고 있으며, 이 지시에 의해 감독관은 공익을 이유로 정보처리기관의 정보보호원칙 이행 의무를 면제할 수 있다.

아시아-태평양 지역의 전반적인 정보보호 경험을 살펴보면, 부문별 규약은 그다지 중요하지 않으며 제정된 사례도 거의 없다.

이행현황의 평가를 위한 감사 및 점검 실시

정보관리자의 법규 이행을 평가하기 위해 DPA가 실시하는 정보관리자 감사는 이 지역의 정보보호관행에서 찾아보기 힘들다. 호주 연방법에서는 감독관에게 공공부문 기관의 이행을 감사할 수 있는 권한을 부여하고 있지만, 감독관은 예산상의 제약을 이유로 모든 감사 활동을 포기하여 왔다. 호주 법개혁위원회(ALRC 2008:47-6)는, 사생활보호감독관에게 공공부문기관이 보유하고 있는 개인 정보에 대해 '사생활보호 실적 평가(Privacy Performance Assessments)' (가령, 감사)를 실시할 수 있는 권한을 부여하여야 한다고 권고하고 있다. 호주의 기타 DPA는 감사권한이 없다. 홍콩의 감독관은 '공식 점검(formal inspection)' (s. 36)을 실시할 수 있으며, 점검 결과를 바탕으로 하여 해당 정보사용자 집단에게 권고하는 내용을 보고서로 발표할 수 있다 (s 48(1)). 그러나, 이러한 권한이 사용된 적은 없다. 감독관은 자발적인 내부 감사나 '사생활보호 이행 감사(PCA: Privacy Compliance Audit)'의 활성화를 제안하여 왔으나, 활성화를 보여주는 증거 자료는 없다.

감사권한을 지닌 DPA에게는 그 결과의 공표 여부를 결정할 수 있는 권리뿐만 아니라 적어도 이행상 중대한 문제점이 발견된 경우에는 그 결과를 공표하여야 하는 의무도 주어지는 것이 바람직하다. 그러한 공표 의무가 없다면, 감사 활동이 대응적 규제에 기여할 수는 없을 것이다.

사생활영향평가(PIA: Privacy Impact Assessment) 실시

이 지역의 DPA는 PIA와 관련된 기능이 거의 없다. DPA가 법제에 의해 촉발된 상황을 근거로, 또는 장관의 요청에 따라, PIA를 실시해야 하는 구체적인 요건도 없다. 또한, 이 지역의 DPA는 문제를 발생시킬 수도 있다고 판단되는 예정된 또는 현행 정보체제에 대해 PIA 실시 여부를 결정할 수 있는 구체적인 권한도 없다. '소송경계 의뢰서(watching brief)'

를 유지하고 기술적 변화에 대해 보고하는 권한과, '자체 동의' 조사를 실시할 수 있는 권한은 DPA가 PIA와 유사한 활동을 할 수 있게 하는 권한으로 해석되지 않고 있다.

호주의 법개혁위원회(ALRC 2008:47-4)는, 사생활보호감독관이 (a) 개인정보처리에 중대한 영향을 미칠 것이라고 감독관이 판단하는 새로운 사업 또는 기술 개발과 관련하여 해당 정보처리기관에게 사생활영향평가서를 제출하도록 지시하고, (b) 그러한 지시를 따르지 않는 경우에 장관에게 보고할 수 있는 권한이 주어져야 한다고 권고하고 있다. 이 권고가 안고 있는 문제점은 PIA의 내용이 공표되어야 한다는 요건이 없다는 것이다. 이러한 내용이 민간부문에도 적용되어야 하는지 여부에 대해 5년간 검토해 볼 것을 제안하고 있을 뿐이다.

10. 참고 문헌

[전체 참고문헌 목록은 책자 발행시 대체할 예정임]

Bennett, C and Raab C (2003) *The Governance of Privacy: Policy Instruments in Global Perspective*, Ashgate, 2003

Bygrave, L (2003) *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer, 2003

Georges, M (2009) "History, Structure, and Functions of European Independent Data Protection Supervisory Authorities" presented at Symposium: *Analyzing the Role and Position of an Institution Protecting Individual Privacy*, Seoul, Korea, 30 September 2009

Greenleaf, G (2009) 'Five years of the APEC Privacy Framework: Failure or promise?'(2009) *Computer Law & Security Report* 25 CLSR 28-43

Stewart, B (2004) 'comparative survey of data protection authorities -Part 1: Form and structure'(2004) 11(2) PLPR 46 at <http://www.austlii.edu.au/au/journals/PLPR/2004/30.html>

Stewart, B (2004a) 'comparative survey of data protection authorities - Part 2: Independence and functions'(2004) 11(3) PLPR 81 at http://www.austlii.edu.au/au/journals/PLPR/2004/39.html

Waters, N (2008) 'he APEC Asia-Pacific Privacy Initiative -a new route to effective data protection or a trojan horse for self-regulation?'[2008] UNSWLRS 59, at <http://law.bepress.com/unswwps/flrps08/art59/>

11. 부록 : 아시아-태평양 지역의 정보보호법 개요

아시아-태평양 지역의 정보보호 21년사

Graham Greenleaf, Asia-Pacific Editor

2009년 8월 Privacy Laws & Business International Newsletter 100호 pp. 21-24에 게재

Privacy Laws & Business가 출간된 21년의 기간은 아시아-태평양 지역의 정보보호 변천사와 거의 정확하게 일치한다 (미주 지역의 경우는 다르다). 따라서, PL&B가 성숙기에 접어드는 동안 이 지역에서 정보 사생활 또는 정보보호 법률이 어떻게 발전해 왔는지를 연대기로 개략하는 것이 유용할 것이다. 물론, 헌법적 권리와 민사 및 형사법의 일반 규정들도 사생활을 보호하고 있기 때문에, 이는 전체의 일부에 지나지 않음을 염두에 두어야 한다.

정보보호법의 점진적 성장

아시아-태평양 지역에서 정보보호법을 제정한 곳은 7곳이다. 아직까지, EU는 어느 법에 대해서도 '적정' 여부를 선언하지 않고 있다.

호주의 '1988년 사생활보호법(Cth)'은 연방 공공부문에만 적용되었지만, 이 지역 최초로 OECD 가이드라인에 근거하여 '정보사생활원칙(IPP)'을 완전하게 갖추고 사생활보호감독관실의 설치를 명시한 법이다. 이 법은 1991년에는 신용 보고에 적용되도록, 그리고 2001년에는 민간부문도 포함하도록 확대되었으나, 소위 '소기업 운영인(small business operators, 호주 전체 기업의 90%가 포함될 정도로 광범위하게 정의됨)'에 대한 고용 기록과 정치적 활동 및 언론 활동은 제외되었다. 이 법은 비교적 강력한 시행 규정을 두고 있지만, 사생활보호감독관들이 그러한 규정의 사용을 꺼리고 진정인들이 법원에 항소할 수 있는 규정이 없어서 결과적으로 21년 동안 소수의 감독관 '결정(determination)'과 한 차례의 중요한 법원 판정이 내려졌을 뿐이다. 따라서, 호주의 연방 사생활보호법은 아직까지 잘 알려지지 않은 분야이며, 기관들과 기업들은 그렇지 않음을 입증하는 증거가 없

는 상태에서 이 법의 까다로운 규정들을 선택적인 것으로 취급하게 될 수 있다. 호주의 주와 자치구 거의 대부분이 공공부문에 대해서는 정보보호법을 갖추고 있으며, 일부는 행정 심판소를 통한 보다 효과적인 시행을 보장하고 있다.

일본은 1988년 이후로 공공부문 정보를 관할하는 '행정기구 보유 개인정보의 보유에 관한 법(Act on the Protection of Personal Information Held by Administrative Organs)'을 시행하고 있으며, 이 법은 2003년에 정보 공개에 대한 문서 파일과 처벌을 포함하도록 강화되었다. '개인정보보호법'은 2003년에 처음으로 민간부문에도 적용되었다. '소기업'에 대해서는 데이터베이스에 포함된 직원의 수에 근거하여, 그리고 언론과 기타에 대해, 혼란스러운 예외가 적용되고 있다. 2003년 법에 포함된 OECD 영향을 받은 원칙은 특이할 것은 없지만, 그 해석이 대부분 대상 부문이 서로 다른 24개 부처의 서로 다른 가이드라인에 의해 결정된다는 점이 주목할 만하다. 중앙 법집행기구는 없다. 이 법은 개인 법원 소송권을 부여하고 있지 않기 때문에, 진정인의 소송권 행사 여부는 관련 부처의 시행 및 조정에 달려 있다. 정부 부처의 효과적인 감독을 보여주는 증거 자료는 없다. 소비자 센터와 정부가 연간 접수하는 진정건이 12,000건을 넘지만, 소수의 진정건에 대한 요약 내용이 공개될 뿐이며 이 법의 실효성에 대한 증거 자료는 부족한 상황이다. 이 법은 '인가된 개인정보보호기관(APIPO)'이 진정건 해결을 지원할 수 있는 공식적 역할을 명시하고 있지만, 어떻게 지원하는지에 대해서는 명확하지 않다. 자율 규제 제도인 'Privacy Mark'의 효과도 마찬가지로 알기 어렵다.

뉴질랜드의 '1993년 사생활보호법'은 이 지역에서 최초로 공공 및 민간부문 모두를 관할하고 사생활보호감독관실의 설치를 명시한 포괄적인 법이다. 이 법에 포함된 12개 정보 사생활원칙(IPP)은 상당 부분이 OECD 가이드라인에 근거하고 있으며 일부는 호주의 영향을 받았다. 이 지역에서 가장 효과적으로 시행되고 있는 법이라고 할 수 있다. 감독관이 연간 접수하는 약 650건의 진정 대부분이 접수되는 해에 종료되며, 상당수는 합의에 의해 해결된다. 그러나, 매년 약 20건은 인권심판소(HRRT)에 회부되는데, 인권심판소는 시행가능한 명령을 내릴 수 있는 권한이 있으며 실제로 그러한 명령이 내려지기도 한다. 지금까지 책정된 가장 높은 보상금액은 NZ$40,000이고 그 다음은 NZ$20,000이다. 잘못된 정보

수집, 보안장치 미비, 잘못된 접근 거부, 데이터베이스에 부정확한 정보 보유, 부당한 정보 공개에 대해 보상금이 책정된 경우는 상당수에 이른다. 고등법원과 항소법원에 항소할 수 있는 권리가 있으며, 지금까지 고등법원은 23건을, 그리고 항소법원은 1건을 심리하였다. HRRT와 법원의 판정이 약 200건에 이르며, 그 결과 뉴질랜드는 풍부한 사생활보호법 경험을 지니고 있어서 진정인과 피고소인 모두 법 위반의 결과를 잘 이해하고 있다. 현재, 이 법의 취약 부분인 정보수출제한 규정을 신설하기 위한 개정안이 추진되고 있다.

1995년에 **홍콩** 정부는 '개인정보(사생활보호)령(Personal Data (Privacy) Ordinance)'을 제정하였으며, 이 법령은 공공과 민간부문 모두에 적용되었다. 1997년에 중국으로 '이양'되면서, 홍콩특별자치구는 중국(PRC)에서 최초로 정보보호법을 갖춘 지역이 되었다. 이 법령에 포함된 6개의 정보보호원칙은 OECD 사생활보호 가이드라인과 상당히 일치하지만, 일부 중요한 부분에서는 더 강화된 내용을 담고 있다. 이 법령의 가장 큰 문제점은 사생활보호감독관 또는 (감독관의 결정에 대해 항소할 수 있는) 행정항소위원회(Administrative Appeals Board)가 진정인에 대한 보상금이나 기타 구제책을 정하거나 이를 이행하지 않은 경우에 대해 처벌을 할 수 있는 권한이 명시되어 있지 않다는 점이다. 법원이 보상금을 책정할 수 있다는 조항이 있으나 사용되지 않고 있는데, 그 이유는 그로 인한 비용과 대외 이미지 손상 때문인 것으로 보이며, 따라서 이 법령의 시행은 미미한 수준이다. 결과적으로, 만성적인 정보 유출에 대한 처벌과 진정인에 대한 보상이 이루어지지 않고 있다.

대만의 '전산처리 개인정보보호법(Computer Processed Personal Data Protection Act)'은 OECD 사생활보호 가이드라인의 영향으로 1995년에 제정되었다. 이 법은 제한적으로 적용되어, 공공부문에는 전체적으로 적용되지만 민간부문의 경우에는 8개의 특정 분야만이 포함된다. 감독기구는 없으며, 각 산업 부문의 책임 부처에게 법집행 이 일임되어 있다. 이 법의 시행 또는 실효성을 입증하는 자료는 부족하며, 논평가들은 대체로 이 법이 실효성이 낮다는 의견이다. Yuan 총독은 2000년부터 이 법을 강화하기 위한 대책(적용범위 확대, 원칙 강화 및 엄격한 시행 등)을 제안하고 있지만 아직까지 효과는 나타나고 있지 않다.

한국은 1987년 '6월 민주화투쟁' 이후로 반민주적인 독재 체제에서 자유민주주의 체제로 변화하였다. 2005년에는 인터넷 보급률은 세계 1위에 이르렀다. 이러한 요인들은 한국 국민이 정부 권력의 잠정적 남용이나 인터넷 이슈에 대해 매우 민감하며 정부에게 사생활보호를 강화하도록 요구하는 사회를 만드는 데 일조하였다. 호주, 일본과 마찬가지로, 한국은 먼저 1995년에 공공부문을 관할하는 정보보호법인 '공공기관 정보보호법(Public Agency Data Protection Act)'을 도입하였으나, 이 법은 정부 행정을 관할하는 부처와 정부에 소속된 감독기구에 의해 집행되는 법으로 대체로 그다지 활동적이거나 실효성이 높은 것으로 평가되고 있지 않다. 이 법은 어느 정도 하위부문적(sub-sectoral) 성격으로, 신용과 의료 정보를 관할하는 별도의 법이 별도로 마련되어 있지만, 2001년의 '정보통신망이용촉진 및 정보보호에 관한 법률(Act on Promotion of Information and Communications Network Utilization and Information Protection of 2001, '정보보호법'이라고도 불림)'은 통신망과 컴퓨터를 통해 영리 목적으로 개인정보를 처리하는 개체들에게 거의 대부분 적용된다. 2001년 정보보호법은 OECD 가이드라인의 영향을 크게 받았지만, 2004년에는 정보 위반, 정보 수출과 기타 측면과 관련하여 더욱 강화되었다. '개인정보분쟁조정위원회(PIDMC)'는 민간부문 기관에 의한 법정 사생활보호 위반에 관한 분쟁을 조정하며 조정이 수락되면 시행가능한 금전적 보상을 책정한다. PIDMC는 사생활보호 규정의 위반이 인정되는 거의 모든 경우에 보상금 지급을 지시하며, 시정 또는 기타 구제책과 병행하여 보상금 지급을 결정하는 경우가 일반적이다. 보상금액은 대체로 US$100 ~ US$10,000 수준이다. 홍콩 및 기타 지역과는 상당히 대조적이다. 한국정보보호진흥원(KISA)은 연간 17,000건이 넘는 진정을 접수하고 있으며, PIDMC의 사무국 역할을 담당하고 있다. 효과적인 법집행 때문인지 자율 규제가 기여하는 바는 거의 없다. 2004년 이후로 공공부문과 민간부문에 대한 규정을 포괄적인 정보보호제도로 통합하고 독립적인 감독기구를 설치하려는 시도가 여러 차례 있었으나 성공하지 못했다.

마카오 특별자치구의 '개인정보보호법 (2006)'은 아시아에서 가장 최근에 제정된 정보보호법이며, 잠재적으로 가장 강력한 법에 속한다. 이 법은 (홍콩 법령의 영향도 받았지만) 대부분의 측면에서 포르투갈의 법과 매우 유사하다. 결과적으로, 아시아 지역의 다른 어느 정보보호법보다도 1995년 EU 사생활보호 지침에 가깝다. 마카오가 중국에 속하

는 한 지역이라는 점을 감안할 때, 이는 더 흥미로운 사실이다. 개인정보보호국(OPDP)는 2007년 이후로 이 법을 관장하였으며, 매우 방대한 권한을 지니고 있지만 그러한 권한을 행사하기에는 기간이 너무 짧다.

ASEAN의 잠재성과 중국

정보보호법의 다음 발달 단계는 이미 공식적인 법안을 작성한 여러 ASEAN 국가들(태국, 필리핀, 말레이시아, 인도네시아) 또는 중국에서 목도될 것으로 보인다. ASEAN 회원국은 2015년까지 사생활보호법제를 마련하기로 공약한 바 있다.

태국의 1997년 '공식정보법(Official Information Act)'은 정부 기관과 관련하여 단지 기본적이고 불완전한 정보보호를 제공하고 있다. 이 법은 32명으로 구성된 공식정보위원회(OIC)의 설치와 이 위원회를 지원하는 사무국의 설치를 명시하고 있다. 정보의 자유에 관한 법인 동시에, 개인정보수집과 보유 및 공개를 제한하고 보안을 요구하며 접근과 수정에 관한 권리를 명시하고 있다. 이 법은 사실상 공공부문에 관한 정보사생활 법이다. 민간부문의 적용과 사생활보호 감독관의 설치를 제안하는 여러 법안들이 있었지만, 부분적으로는 현재의 정치적 불안으로 인해 입법에 성공하지는 못했다.

필리핀은 아직까지 관련법이 거의 없는 실정이지만, 2009년에는 상당히 강력한 집행권한과 감독관제를 갖춘 EU식의 법이 제정될 것으로 보인다. 현재, '전자상거래법(2000)'은 기업이 사용자에게 사생활보호, 기밀, 그리고 적절한 경우에는 익명성과 관련하여 선택권을 부여하여야 한다는 일반적 원칙을 정하고 있지만, 이 법이나 일련의 정부 가이드라인은 실효성이 거의 없다. 대법원은 2008년에 법원 규정으로서 '인신보호영장 규정(Rule on the Writ of Habeas Data)'를 채택하였으며 이 규정은 사생활보호 잠재성을 지니고 있으나 아직까지 활용되지 않고 있다.

말레이시아의 사생활보호 현황은 주목할 만한 것은 아니며, 말레이시아의 각료들은 1998년 이후로 포괄적인 정보보호법의 도입을 한 목소리로 주장하여 왔다. 새로운 법안이 2009년에 작성될 것으로 알려져 있으나, 이 법안이 통과된다 하더라도 강력한 정보보

호를 제공할 것으로 기대하는 사람은 없다.

인도네시아의 2008년 '정보 및 전자거래법(Law on Information and Electronic Transaction)'은 전자 매체의 개인정보 오용에 대한 매우 폭넓은 보상권을 명시하고 있지만, 역사가 너무 짧아 큰 의미를 지니고 있지는 않다. OECD 가이드라인가 기타 국제기제의 영향을 받은 법안이 작성되었지만 아직 공개되지 않았다.

싱가포르는 반론의 여지는 있지만 세계에서 사생활보호법이 없는 유일한 선진국이다. 2002년의 '모형정보보호규정(Model Data Protection Code)'은 산업별 자율 규제 규정이지만 그 효력은 알려져 있지 않다. **베트남**은 신설법에서 APEC의 기준을 고려하고 있으나, 기타 ASEAN 국가인 **미얀마, 캄보디아, 라오스, 브루나이**에서는 사생활보호와 관련하여 어떠한 동향도 알려진 바 없다.

중국에서는 EU식의 '개인정보보호법안'이 2007년까지 검토되고 있었으나, 더 이상은 적극적인 검토 대상이 되고 있지 않는 것으로 보인다. 이 법안은 2005년에 중국 사회과학학회 법학부장인 Zhou Hanhua 교수와 전문가들이 중국 정부의 의뢰로 작성하였다. 중국은 개인정보보호를 다루고 있는 국가 차원의 민사법이 존재하지 않지만, 일부 지방정부에서는 부분 조항을 채택하고 있다. 중국 형사법 제7개정조항(2009년 2월)은 매우 다양한 개인정보 공개 및 확보 행위를 위법 행위로 간주하고 있는데, 중국에서 개인정보를 형사법으로 직접 보호하는 최초의 법조항이다. 중국에서 정보사생활권의 확대되면 지역 전체에 강력한 영향력을 행사할 것이다.

동아시아 지역의 현황을 마무리하기 위해 독특한 노선을 따르고 있는 몽골을 살펴보면, 1995년 '개인비밀유지법(Law on Personal Secrecy, 즉, 사생활보호법)'을 채택하였으며 이 법은 다양한 유형의 개인정보에 적용되며 위반 행위 고소 및 예외 규제의 권리를 부여하는 여러 법에 영향을 미치고 있다. 관리들에게 서약을 하게 하는 등 관리를 대상으로 훈련을 실시하고 있다.

인도, 아웃소싱, 그리고 남아시아: 완강하게 버티는 지역

남아시아는 아시아에서 정보보호에 있어 '최후의 개척지'라 할 수 있지만, 현재 이곳의 상황은 급변하고 있다. SAARC가 사생활보호에는 거의 관심을 보이고 있지 않은 점을 감안하면 지역 협약이 그 원인일 가능성은 낮으며, 그보다는 유럽으로부터의 상업적 압력이 요인일 것이다.

인도는 아직까지 이렇다 할 정보보호법을 시행하고 있지 않다. 2000년 '정보기술법(Information Technology Act)'은 정보보호는 그다지 중요하게 다루고 있지 않으며, 아직까지 시행되고 있지 않다. 이 법의 2008년 개정조항은 '민감한' 정보의 공개에 대한 구제를 명시할 수도 있으나, 어떠한 규정이 작성되는지는 두고 봐야 할 것이다. 2005년의 '정보신용기업(규제)법(Credit Information Companies (Regulation) Act)'은 잠재적으로 중요한 포괄적 신용보고규정이지만, 여전히 인도준비은행(Reserve Bank of India)에 의해 효력이 부여되고 있다. 정보보호와 관련하여 인도에서 효과적인 부분은, 2005년의 '정보권법(Right to Information Act)'에 의해 인도의 어떠한 공공기관이 보유한 개인정보에 대해서도 주어지는 접근권을 들 수 있다. 이 법은 적극적으로 시행되고 있으며 이미 상당한 분량의 판례법이 축적되었다. 인도의 대법원이 이전에 정보권법의 경우에도 그러하였듯이, 사생활에 대한 헌법적 보호를 강화하여 정부로 하여금 정보보호를 명시한 법을 제정하도록 압력을 행사할 수 있을지는 알 수 없다. 효과적인 자율 규제를 보여주는 증거 자료는 없다.

SAARC 지역의 기타 국가들(**파키스탄, 방글라데시, 스리랑카, 네팔, 몰디브, 부탄**)에서는 정보보호동향이 전혀 감지되고 있지 않으며, 다만 몇 년 전에 파키스탄에서 여러 관련 법안들이 제출되었으나 시간 경과로 효력이 소멸되었다.

결론: 다양한 영향하에서 점진적인 입법의 가속화

지난 21년간의 정보보호 동향의 간략하게 살펴본 결과, 여러 가지 사실이 드러난다. 정보보호원칙에 가장 큰 영향을 미친 것은 OECD 가이드라인과 EU 지침이며, APEC의

사생활보호 기본틀은 아직까지 직접적인 영향을 미치고 있지 않다. EU 지침의 영향력은 시간이 경과함에 따라 더 크게 작용하고 있다. 유럽에서 일반적인 모형이며 아시아 지역 최초의 관련법(호주)에도 포함되어 있는, 중앙 차원의 사생활보호감독관에 의한 시행/관리 모형이 여러 곳에서 채택되어 왔지만(뉴질랜드, 홍콩, 마카오의 법과 태국, 필리핀, 한국의 여러 법안), 그 실효성에 대한 증거가 거의 없는 시행책임분산 모형(model of diffuse enforcement responsibilities)도 북아시아 국가들에서 발견된다(일본과 대만의 법, 중국 법안). 감독관의 사례 연구나 심판소/법원의 판정이 상당량 축적되어 해당 법이 적절하게 해석될 수 있는 발달된 법집행 구조를 갖춘 곳은 거의 없으며, 뉴질랜드는 대표적인 예외에 해당한다.

전반적으로 볼 때, 정보보호법은 아시아-태평양 지역 전체에 지속적으로 확대되고 있으며, 현재 법안의 절반이 법으로 통과된다면 그 속도는 빨라질 것이다. 기존법은 계속 강화되고 있으며, 이 지역 내 정보수출제약은 더욱 확산되고 있다 (호주, 마카오, 한국, 홍콩(미발효), 뉴질랜드(예정)). APEC의 기준이 원칙의 직접적 채택이라는 측면에서는 거의 영향을 미치지 못한 것으로 보이지만, 정보보호에 대한 관심과 입법 노력은 배가시켰을 것이다. 이 지역에 미치는 외부적, 내부적 영향에 의해, PL&B가 또 다른 의미 있는 날을 맞이하기 전에, 정보보호는 아시아-태평양 전역에서 법제의 한 요소로 인정받게 될 것이다.

발표 2

유럽의 독립적 정보보호 감독기구의 역사, 구조 및 기능

Marie GEORGES (Informatics and Liberties Consultant)

2
발 표

History, Structure, and Functions of European Independent Data Protection Supervisory Authorities

Marie GEORGES (Informatics and Liberties Consultant)

Let me first thank the National Human Rights Commission of Korea for the opportunity to participate in this symposium with so many distinguished people from one of the most advanced nations in information technology. I am pleased to be able to share with you thoughts from my many years of experience in French, European, and international data protection and privacy activities. I have been involved in these matters from the emergence of privacy in the 1970's until my recent retirement from the staff of the French data protection authority.

Thank you also to Korea for this opportunity to come back to Seoul. I was here in 2002 for a conference at the invitation of the KISA. I am pleased to be able to meet again with colleagues from KISA and from NGOs, including some I met at conferences of the International Data Protection and Privacy Commissioners. KISA has been accredited to participate in these conferences since 2004.

Institutions designed to protect individual data protection and privacy rights originated in Europe during early stages of computerization of society in the late 60's and first half of the 70's. These oversight institutions were established by law to limit the undue power that could be gained through the processing of personal data and to protect the rights of individuals. They are generally referred to internationally as "Data Protection Authorities"[1] (DPAs), or "Data Protection Commissioners". In France, the data protection authority is called "Commission for Informatics and Freedoms." This title indicates that the jurisdiction of the

1) "Data Protection" is the English translation of the word ("Datenschutz") the Germans use to designate the new area of human right.

French authority is wider than privacy, and this is also true elsewhere in Europe. We will come back to that later.

DPAs require independence for their work. This is true in Europe and elsewhere around the world. Independence is important for any sustainable data protection system because innovation and deployment of IT have become an essential part of almost any human activity. There is a correlative need to insure the preservation of data protection rights in order to insure the stability of democratic values. As the world struggles to recover from the current international crisis, in part through the expanded use of IT, that need is even greater.

Introduction: History and brief general state of play

Before getting into details of the reasoning behind the structure, functions, and independence of DPAs, and the state of play in the EU, let me outline some relevant history and some future next steps.

Historical dates

1970 The Lander of Hess in Germany adopts the world's **first general DP law for the public sector**, following a public debate about a plan to centralized personal data processing for several government departments in a common computer center. The law establishes **an independent supervisory authority.**

1973 Sweden adopts **the first comprehensive DP** law in the world, **covering both public and private sector** files of personal data. The law also establishes an independent DP authority.

1978 France adopts a comprehensive DP law, creating **the first independent, collegial, and pluralistic DP authority** in the world. The legislation came after a major press campaign against, in particular, the SAFARI project, which aimed to turn the Social Security Number into a unique identifier from birth to death as a cost effective management tool for the public

sector. The law passed after a parliamentary battle in both chambers of Parliament in which both majority and opposition Members fought against the Executive Branch to keep the DPA under its control. The Parliament added also for the first time in the world coverage of **manual files** to avoid circumvention of the law.

1979 The German DPA hosts the **first international conference of DPAs** in Bonn. This started international cooperation among national DPAs and increased their influence on the international level.

1981 To insure free flow of data among its members while insuring the DP rights, the Council of Europe adopts a **binding convention** (n°108[2]). Its need comes up in parallel with the adoption of the first of national laws and its adoption take place some months after the US delegation, unwilling to support the adoption of a binding instrument, leaves the negotiation to initiated instead a parallel **OECD** effort, which adopted late 1980 **non-binding guidelines**[3]. The **principles set out in these instruments are similar to each other and are** close to the **Fair Information Principles elaborated in the US in the** early 70's**.** However **the Council of Europe Convention**, which is open to third countries, is **the first binding international instrument that reinforces rules for the processing of so-called sensitive** data in order to prevent discrimination. None of these instruments requires the establishment of a DPA. The CoE convention was updated on this point later.

1991 On the basis of the report of a judge who took part in the drafting of the CoE convention and the OECD guidelines - and who had formerly served as the first head of services for the French DPA - the General Assembly of **UN adopts unanimously the first worldwide "Guidelines for the regulation of computerized personal files"** (resolution 45/95 of 14 December 1991) covering both private and public sector. The UN guidelines are consistent with the OECD guidelines and the Council of Europe Convention 108, including coverage of sensitive data. The UN Guidelines are the **first international standard that includes an**

2) Convention for the protection of individuals with regard to automatic processing of personal data n° 108 of 28.1.1981

3) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Independent DPA provision in point *8 on* supervision and sanctions: "The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies". However, the UN instrument is not binding.

1995 On the initiative of the German DPA during the international conference of DPA in Berlin in 1989 and with support from the French DPA, the European Commission proposes a legislative directive for harmonizing national laws which is adopted by the European Parliament and the Council for a on October 25, 2005[4]. **The Directive** covers digital and manual data processing in the private and the public sectors in all areas where community law is competent. It draws upon the Council of Europe Convention. A major purpose is the harmonization of national laws in the context of the common market. It is, on the international level, the **first regional binding instrument providing for national mandatory independent DPAs and for cooperation between national DPAs.** The EU DP Directive also includes **a binding clause related to transfers of data outside EU territory, requiring adequacy of the protection in the third country or at least sufficient guaranties presented by the foreign recipient**. **It provides for exchange of data about investigations of transnational data processing.** It also establishes for first time **a regional body** whose members include the national **DPAs** and the DPA for EU institutions.

2003 Two years after having adopted its the well-known worldwide cybercrime convention to which a number of non-European states already ratified, the Council of Europe adopts a protocol to the **Convention 108** making mandatory the setting up of DPAs and providing for

4) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *Official Journal L 281 , 23/11/1995 p. 0031 - 0050*

similar provisions related to transfers of data to third country. While the Convention has been open to third countries since 1981, no third countries have yet ratified it.

2001 to 2009 The 22nd international conference of DPAs, hosted in Paris, adopts **rules covering accreditation of DPAs** with the view of being able **to adopt international resolutions** with legitimacy. In 2005, on the eve of the WSIS, the 27th conference adopts a resolution **calling in particular for the UN and the Council of Europe to set up a binding international instrument of worldwide scope**. Because of the lack of data protection activity at the global level while the international nature of data processing continues to expand, **the 31st international conference of DPAs meeting in Madrid next November, intends to recommend a more elaborate international minimum standard scheme, including national law provisions that would call on DPAs to cooperate internationally for enforcement of law**.

Brief State of play in the world:

Over 50 countries in the world, including countries on all continents, have adopted DP laws. In many other countries, DP initiatives are currently under consideration.

It is now unusual for a DPA law or draft not to include a DPA. Where it does not, thee need for a DPA is repeatedly raised in public debates and parliamentary initiatives.

It is also unusual now that an established DPA does not have oversight functions for both the public sector and the private sector. In remaining countries, some institutions have data protection competence over a part of the private sector. For example, in the US, the Federal Trade Commission has limited authority over parts of the private sector based on laws related more to consumer rights than to human rights. In the US, starting in 1974, there have been occasional proposals in the Congress for an independent data protection authority, but without success to date.[5] Instead, we see the development of internal oversight mechanisms within specific government agencies at the federal level (but lacking in independence) or voluntary

5) See Robert Gellman, Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions, VI Software Law Journal 199 (1993)., http://bobgellman.com/rg-docs/rg-softwarelj.pdf; A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board, 54 Hastings Law Journal 1183 (2003)., http://bobgellman.com/rg-docs/Gellman-Hastings-03.pdf.

privacy officers in private sector companies.

In the EU, the harmonizing directive of 1995 and its implementation in the Member States have led to the establishment of independent DPAs in all its 27 members states, in the 3 States members of the Economic European Area, and in the 2 States that are currently candidates to accession. Those DPAs are competent nationally over both private and public sectors and over transfers of data outside EU. DPAs also have enforcement powers and participate in an influential advisory group at the European level.

The existing incomplete international system of DP regulation is the subject of new initiatives from individual DPAs and from the international conference of DPAs with the goal of facilitating both the adoption of national laws based on international standards and the establishment at the international level of more coordinated regulatory and enforcement mechanisms

***

To cover my topic, and partly because I am not an academic, I chose to answer to a specific set of questions to describe the state of play in EU and in some other countries with which I have had some experience, especially in Africa and in South America. The questions are:

- Why a DPA? What are the necessary functions, including on international level?
- Why should a DPA have authority over both the public and the private sector? Why DPAs may need other human right competences and which ones?
- Why should a DPA be independent, and how to achieve independence?

I- Why a DPA? What are the necessary functions?

I-1. The general nature of data processing risks and of the corresponding DP principles: the need for promoting balances and for insuring compliance

The general risks that digitized personal information held by third parties present to the concerned individual are quite well known: data are easy to copy, to pass on to others, to be lost or destroyed, to be kept for years at very low cost, to be reused without knowledge or consent for purposes other than the one for which they were collected, and to be used for making decisions automatically on the basis of personal or statistical profile.

Having identified those risks as early as the 70's, experts from both sides of the Atlantic developed a set of basic principles defining specific obligations for those processing personal data and specifying rights for individuals. The EU implementation of those principles, which is more detailed than other international documents, provides (together with more details):

- Responsibility and the transparency principles, prohibiting data activities that may reinforce unduly the power of the controller (the person conducting the data processing) of personal data without notice to data subjects;
- Legitimate purpose and the incompatible purpose principle that prohibits abuse, reuse, or matching of personal data for a different purpose without the knowledge or agreement of the data subject (right to object or to consent);
- Proportionality (or minimization) principle, prohibiting both collecting unnecessary data and keeping data when no longer needed;
- Reinforced rules in case of dealing with "sensitive " data
- The adequacy of the level of protection provided in a third country where personal data are intended to be transferred
- Security principle ;
- The right of the individual to be informed, to access to his/her data and to have data corrected, completed, or suppressed where necessary; to know the origin of the data; to object to a processing on basis of a legitimate ground; not to be subject to automated decisions based on profiling without safeguards;
- Tailored derogations from certain principles for crucial public interests may be adopted on the basis of constitutional criteria when necessary in a democratic society, publicly available and clear, adopted by the legislative branch.

These principles are characterized by their general nature, not tied to a particular technology or context. At the same time, the interest of those persons processing data, private or public, may well conflict with the principles. These conditions create both some uncertainty and some temptation.

There is a need, therefore, for external oversight from impartial, qualified, and experienced persons to help strike a proper balance (i.e., what is a legitimate purpose? what is a proportional response?). Moreover, taking into account the volume of data processing and the number of individuals affected, this need has to be met in a more responsive and detailed way than a Parliament or a Justice institution could possibly provide.

In the EU, the choice has been made to rely on a multi-dimensional system, mostly in the hands of DPAs, aimed at ensuring efficiency. Major include by reference to the DP directive of 1995:

- transparency of all data processing through notification to the DPA (with exceptions based on regulations or on the presence of a Privacy Officer, article 18) aside transparency insured with regard to concerned individuals (information at the time of collection of data..);
- a prior opinion by the DPA (checks and balances) or Parliament on projects that present specific risks for human rights in both public and private sectors (article 20, 28) ;
- a review by the DPA of codes of conduct drafted by sectors representatives of industry to make sure of conformity with the law (article 27)
- DPAs'power to investigate and, left to the choice of the States, to impose sanctions and provide remedies. DPAs in Europe can hear claims, are empowered to investigate, to deliver injunction, are able to resolve cases by informal mediation (for over more than 90% of claims) and, left to the choice of States, to provide, in case of violation, sanctions and remedies (administrative fines i.e. by DPAs in France, Greece, Italy, Netherlands, Spain, and remedies by DPA in Italy) or to bring cases to the Court;
- individuals retain the possibility of taking a complaint to the Courts (articles 22-24 and 28) ;

- DPAs'power to issue opinions on bills related to data processing, in particular aiming to derogate from DP principles, and on governmental regulations.

All decisions taken by DPAs can be appealed through the courts, see article 28 (i.e., in France through the Supreme Court)

This is not to say that the EU situation is already idealistic. When implementing the directive, the Member States may have chosen an over bureaucratic system, or on the opposite did not gave sufficientreally effective powers to the DPA in on or another field.

However, the combination of the different powers and the free speech they are entrusted with, allow DPAs to make public their criticism over any policies which affects the DP rights in both private and public sectors

I-2. The growth rate of IT innovations: the need for stimulating DP culture, for monitoring, for particular recommendations, for influencing technical development, for alerting Government and Parliament to the need for additional tailored rules or policy.

New types of IT innovation are often led by new actors, designed for new purposes, and deployed in new sectors or for new functions for the benefit or at the risk of specific populations. For example:

Mobile location data, technically collected for connecting calls, are suddenly offered by telecom operators for the new purpose of locating family members or employees and/or for commercial purposes;

Social networks designed for a closed population suddenly offered to all population without default, appropriate, and privacy-friendly functionalities;

Biometrics systems based on those used for police matters offered for a new use,

namely recording working hours

Radio frequency identification technology, originally designed to manage the distribution of pallets of goods, is used in mandatory ways for border control, passports, and similar activities without adequate protections.

Because of the novelty of these uses of technology, concerned individuals and opinion leaders may be unaware of their implementation. Those who seek to profit from the new uses may not be paying attention to the social/freedom risks and consequences of the technology, and they may not properly apply DP principles.

More generally, IT innovations are characterized by a multi-evolutionary and expanding nature which structure heavily the society, including high growth rates, new functions, lack of transparency, integration in all kind of objects, invasive activities (e.g., collection or use of internet protocol addresses, video surveillance, biometrics, RFID, DNA), faster deployment in applications, and connections to more daily activities from even before birth to after death. In response, a multi-dimensional system of DP functions is permanently needed and, in the EU, this response comes from the DPAs, who can act on their own initiative. For example, DPAs can:

- stimulate DP culture by encouraging the development of greater DP awareness, using communication by radio, TV, internet, conference, speeches in professional forums, partnerships (i.e., in France, with the Ministry of Education, with university presidents for introducing DP courses, etc.) ;
- monitor IT evolution, foresee uses, and influence research activities and technical standardization bodies;
- give advice;
- adopt and disseminate recommendations based on experience and after consultation with the representatives of concerned professions and people i.e. the French DPA's recommendation on how to preserve free speech on web forums (no need to publicize the authors' names of messages but to establish a mediator to insure the messages made public are not infringing the constitutional limitations i.e. publicity in favor of nazis activities), or its recommendation on how to use biometrics in a proportional way, such

as allowing a biometrics system employing fingerprints to be used only in a high security risk context and not for recording an employee's hours of work.

- monitor the application of those recommendations, and if the advice is not followed, alert the political level (government and parliament) of the need for additional tailored binding rules (i.e., in France, biometrics systems being considered as presenting risks for freedoms and the recommendations not being sufficient, most applications must now be approved in advance by the DPA).

The means required for operating those functions are very high and time consuming, that is why cooperation between DPAs at the EU level appears to be the best way to keep up dated policies

All these functions will be needed even more because of the coming nanotechnologies that some predict will be used widely in data processing.

I-3. Complementary legal tools and emerging functions: "Personal data protection official (privacy officers)" and certification

In order to insure efficiency in a context of exploding personal data processing activities, two main additional tools are being considered for future application within the EU: the "Privacy officer function" within entities that hold personal data, and certification.

Personal data protection official (privacy officer)

Taking into account that many personal data processing activities do not present particular risks when professionally performed (over 80%), the EU Data Protection Directive provides for a choice to be made by Member States between two equivalent exceptions from the notification requirement to the DPA (article 18). The first is when a personal data official

(called in France “correspondent for informatics and freedoms”) is designated by the data controller responsible for the personal data processing, an approach that originated in Germany. The second is on the basis of regulations adopted by the DPA that specify the main features of allowable data processing (purposes, concerned persons, list of process data and recipients), an approach adopted originally by Sweden, France and Netherlands.

Several Member States when implementing the Directive provided for establishing privacy officers, on a mandatory or on a voluntary basis (i.e., Netherlands and France). This approach may be adopted more broadly within the EU in the future.

Certification

The technology that provides new features, protocols, products and a growing number of data preprocessing services - much of which has become an essential element of the daily lives of many individuals - has raised in the EU questions about the benefits of a certification scheme

The State of Schleswig Holstein in Germany has been the first to provide a procedure for DP certification to supplement the lack of a priori control. The certificate is delivered by the DPA on demand and at the expense of the entity willing to get such certificate. The products or services are evaluated in advance by independent experts chosen from a list of accredited experts.

A European research project for an EU certification scheme is on the way, coordinated by the Schleswig Holstein’s DPA and in which the French and the regional Madrid DPA are involved.

The French DP law provides already such an approach and gives the power to the DPA to issue certificates. This authority has not yet been implemented.

Outside the EU but in Europe, the Swiss DPA already issues certificates. A number of DPAs in EU Member States are raising the need to examine this approach for the future.

I-4. International cooperation functions

As more and more personal data processing and services are of transnational nature (e.g., Internet web sites, outsourcing diverse activities, ubiquitous computing, transfers of data to other States authorities), as are innovations in IT (internationalization of production and distribution of IT products for personal data processing or that use personal data i.e., such as biometrics captors), many functions of DPAs at national level are in need of greater coordination at an international level.

Up to now, only in the regional area covered by the EU are these functions institutionalized at the EU level. There is no international global level coordination based on coordinated independent oversight bodies. But on international level, the DPAs have been organizing themselves at their own initiative and with their own means in a more and more influential network since 1979. However they won't be able to cooperate by exchanging data related to investigations on common cases until bilateral (and, more efficiently, multinational) agreements entrust them with the power to do so, along with the appropriate democratic guaranties for the concerned persons.

I-4.1. Regional DPAs' functions and methods at the EU level

When hearing claims and conducting investigation, functions which are enforced at national level, DPAs must cooperate by using their powers on their territory for the benefit of another DPA, which may be competent according to the law applicable to transnational data processing (article 28.6.of the general directive of 1995).

In addition to their national competence for monitoring IT and for DP regulation, DPAs are empowered within the institutionalized network they form at the EU level, under the name of "Working Party on the Protection of Individuals with regard to the Processing of Personal Data." The Working Party, established by Article 29 of the EU Directive (commonly called the Article 29 Working Party or WP29), has broad powers to initiate and adopt any needed recommendations, and to undertake the following missions of a consultative nature for the

European Commission (article 30):

- To contribute to the uniform application of the directive provisions,
- To give an opinion on the level of protection in the Community and in third countries; The Article 29 Working Party gives its opinion on whether a foreign country insures an adequate level of protection so that personal data can be transferred to a recipient located there. The European Commission has the power to find that a third country does not ensure an adequate level of protection (Article 25).

In order to set up a general policy on adequacy, the WP issued a series of coherent, flexible, and detailed papers on how to evaluate adequacy and on how to interpret and grant the derogations provided in the Directive. In particular, transfers of data to recipients located in a non-adequate country may be allowed if there is sufficient protection stipulated in contracts or if there are so-called “binding corporate rules” that recognize EU DPA enforcement power. WP29 papers on these subjects became the basis for further European Commission evaluation and for decisions taken on a national level.

- To advise on any proposed amendment of the Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data, and on any other proposed Community measures affecting these rights and freedoms;
- To give an opinion on codes of conduct drawn up at Community level.

All of the over 150 working documents, opinions, recommendations, and working papers of an interpretative nature adopted by the Working Party are public. Some of the most influential WP papers cover the concept of personal data, application of DP principles to the Internet, e-government, employment data processing, video-surveillance, RFID, biometrics, search engines, and social networks. See http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

When adopting its papers, the Working Party hears from representatives of concerned persons and undertakes online consultation on the drafts.

The Working Party elects a chairman and a vice-chairman, meets more than four times a year, adopts a yearly program of work, and creates subgroups where necessary. The European Commission unit responsible for Data Protection operates its Secretariat.

The Working Party is also invited by the European Commission to participate in groups aimed at drafting policies. For example, after the Working Party issued its 2005 paper on RFID, it participated in the group that, during 2007 and 2008, drafted the recommendation on RFID that the Commission adopted on May 12, 2009 (providing for a prior privacy assessment of RFID application by providers reviewed by national DPAs, deactivation by retailers at point of sales of tags unless consumers give their informed consent to keep tags operational and calls on the EU standardization body to develop logos for transparency of RFID tags and readers [6]).

The WP also increasingly serves as an advisor to the European Parliament. For example, the WP provided advice about the request by the United States and other countries for disclosure of passenger name records (PNR) used in air line reservations systems. See Professors in Law Y. Poullet and S. Gurtwirth's article, Belgium on the Article 29 Working Party's role in the DP governance in EU[7].

I-4.2. The cooperation within the International Conference of DP and Privacy Commissioners

Because of the novelty of their institutions and the similar nature of the problems they face nationally, DPAs looked for opportunities to exchange views bilaterally and, as early as 1979, at a multilateral level. The first international conference of DPAs, which has become a yearly

6) http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

7) The contribution of Article 29 Working Party to the construction of a harmonizing European data protection system ; an illustration of « reflexive governance », Prof Yves POULLET, director of the Crid, Faculty of Law, FUNDP, Namur, and Prof.S.GUTWIRTH, Law, Science, Technology and Spciety, Faculty of Law and Criminology, Vrije Universiteit Bruseels, Belgium

event, was hosted by the federal German DPA in Bonn, Germany.

The need for continuing support for their national positions, which may be challenged at home or abroad, together with the growing need for common positions on ever-increasing transnational transfers of data, services, and sector rules adopted by international organizations for the processing personal data (i.e., ICAO, ISO), led the DPAs at an international level to adopt resolutions on matters of common interest. See, for example, the resolutions adopted at the last international conference hosted by German and the French DPAs in Strasbourg, France in 2008, concerning. the online protection of children, social networking, and setting international standards on privacy and personal data protection (www.privacyconference2008.org).

The adoption of resolutions has been possible since the DPAs approved in 2000 (Italy) rules on how to introduce draft resolutions (requiring support from at least three DPAs and at least one month before the conference) and on who may participate and who may vote in 2001, France, (requiring approval by an accreditation committee that prepares a report and draft resolution for the general assembly). DPAs are allowed to vote if they are national DPAs established by law with independent status, if the DP rights they oversee are consistent with international principles found in the OECD, UN, COE or EU DP standards, if their authority is not limited to consultations alone, and if they have jurisdiction over competence over a large range of activities. Non-accredited DPAs are observers, and subnational DPAs are allowed to participate in debates.

The international conference still does not have legal status or a permanent secretariat. The secretariat is operated by the DPA that last hosted the international conference. Subcommittees established by resolution undertake continuing work on topics of common interest, such as on the question on how to set up a permanent web site (not yet operational), or on to achieve recognition as an international organization that addresses DP matters (ONU, CoE, OCDE, ISO…).See www.privacyconference2008.org,

The annual international conference of DPAs is mostly conducted in public, and individuals, organizations, and companies from all over the world may attend. Only a small part of the conference is closed to for consideration of internal affairs.

I-4.3. Particular initiatives taken by EU DPAs in order to promote DP laws in countries speaking the same language: more successes

Since the year of the World Summit for Information Society (Tunis 2005), the international conference of DPAs (Montreux, Switzerland, 2005) has been pressing governments, the UN, and the Council of Europe to promote data protection rules on global level though an international convention of global scope, so far without success. The UN Commission for Law did not designate a reporter. However, the CoE said last year that it is willing to contact countries to promote the Convention 108 and its protocol. A process for developing an international instrument or for promoting the COE Convention would promote efficiency on global level and would create an incentive for countries without a DP regime to adopt one.

Progress has been achieved when DPAs have undertaken direct initiatives with countries speaking the same language. Spanish, Portuguese and French speaking DPAs are promoting DP by sharing their experiences with countries which have no DPAs. Successful collaborations have been undertaken with Mexico, Uruguay, Macao, Morocco, Burkina Faso, Senegal, and Benin. At the suggestion of their DPAs, corresponding language international organizations are now providing assistance following declarations at summits of Head of States supporting the development of DP rights and cooperation among DPAs. Notably, the French Speaking International Organization ("Organisation Internationale de la Francophonie", OIF), which supports international meetings and regional conferences on DP , will help by holding a regional conference in November 2009 in Hanoi on IT and law, and in particular on DP rights and on the Freedom of information. That conference, organized by the Maison du Droit with the support of the French Speaking association of DPAs, will bring together experts in IT and Law and representatives of all concerned parties and institutions (government, parliament, courts, industry and social society) from the four members and observer States of OIF (Cambodia, Laos, Thailand and Vietnam).

II- Why is a DPA for both private and public sectors necessary? Why combine DPA oversight functions with other human right oversight functions, and which other functions?

Several reasons militate strongly in favor of a DPA with authority over both public and private sectors, including the need for more consistent rules for the benefit of citizens, the need for better coordination with others human rights activities, and the need for greater efficiency in the conduct of an independent authority for DP.

II-1. Why is a DPA for both private and public sector necessary? For consistency of rules and protection of individual rights

Both sectors use the same technologies

While public and private sectors pursue different goals and conduct their activities in different ways, both use same technologies. Each sector may be the center of innovations that may later be used by the other. For example, computers originated in the military sector and then spread to the governmental and private sector. The Internet also started with the military, spread to international research activities, and then to international commerce. RFID originated mostly in the private sector and is now spreading to the public sector.

Same activities/IT applications can be found in either sector

The same core activities take place in education and in the health sector, whether the organizations are public or private. That leads to the same kind of personal data processing, which may even be interlinked. A public hospital may share digital facilities with private physicians. Networked systems of medical records established under public policies may be operated by private companies and may support medical professionals operating in public or

private facilities. Similarly, both public and private sectors operate human resource management systems that use the same technology and raise the same DP concerns.

What if the DP guaranties are not the same in both sectors?

Uses in one sector of data originated in the other

Enterprises may be under the obligation to transfer data (e.g., on employees to a public social security agency or to a tax revenue administration). Public authorities may use publicly available telephone directories or other resources created by private companies.

There are many routine transfers of data between sectors. There are also delicate issues, which are intensifying with the digitalization of data. For example, private entities seek to use public records for other purposes, and public security authorities want online access to airline reservation systems, to telecommunications records, and to internet service providers records.

Conclusions

Because of data sharing, there is a crucial need for coherence in the application of DP principles in order to avoid loopholes that undermine rights of data subjects. Without consistent application of principles, basic concepts may be interpreted in different ways by the public and private sectors. Records created in one sector subject to specific protections may lose those protections if transferred elsewhere. If a matter under investigation by one DPA crosses both sectors, the DPA will not be able to function successfully without jurisdiction over both sectors.

Of course, some differences in the application of DP principles may be legitimate in certain cases, but only after proper consideration can an appropriate solution be implemented.

II-2. Why it is possible to combine DPA oversight functions with other human right oversight functions, and with which? Coherence and efficiency

Some human rights other than DP also need to be overseen by an independent authority.

This is in particularly true for the right of access to public information or documents in the private sector. Some countries have experience in establishing a single independent institution that combines oversight of DP and of the right of access.

II-2.1. The fundamental right to access to public information or document oversight function sometimes combined with the DP one

This combination of fields of competence started in Canadian provincial governments where the right to public information was established before the DP right (i.e. Quebec and others provinces). It is now developing in Europe in some countries where the access right was recognized after the DP right, such as in the UK, Germany and Switzerland. In France, the right of access to information was established in the same year (1978) as the DP right, but two different independent authorities remain, despite some debates. However, a recent reform in the access law seeks to insure more coherence by requiring the chairman of the DPA to designate one member of the independent Access Authority.

The access right to public information by citizens includes exemptions, in particular for preserving the privacy of an individual who is not the requester, while it insures access by an individual to information about himself or herself. The right of access under DP principles is the same as the right under access principles.

Public information, whatever its content, is increasingly computerized, and pressure grows to give online access to public data for new public or private services. This raises additional issues that call for greater coordination between DP and access regimes. Third party requests for information under access laws may create conflicts with rights under DP rules.

II-2.2. Mediation as ombudsman between citizen and public administrations

The institutional solution which combines access and DP oversight functions with an Ombudsman function can also be found in smaller jurisdictions, as is the case in the Province of New Brunswick in Canada (300 000 people). It in the future, this could be an effective

solution for developing countries with limited resources.

III- Why the Data Protection Authority has to be independent? How to achieve independence?

III-1. Why independence? The nature of the functions and the more and more fundamental recognized nature of the DP right

Two main related reasons show the need for impartiality and independence from government.

The first, as seen above, is the need for faster and more efficient way to operate rather than relying on the two other independent institutions for the government which are the Parliament or Justice. As a matter of facts DP activities are of a such nature that in a democratic society need to function in an impartial and therefore independent way:

- they imply criticizing where pertinent in particular government when issuing opinions on policies or authorizations prior to the establishment of certain data processing,
- after the fact, they conduct investigations, provide mediation, and impose or look for sanctions in case of serious violations of rights, functions that require impartiality, independence, procedures guarantying the rights of defense.

The second related reason is that the human rights nature of the data privacy right is more and more recognized at the highest level of legal norms, together with its interrelation with other human rights, in Europe and in other continents.

In the Information Age, the DP right provides a safeguard for the exercise of the other fundamental rights.

Which trade union, association for human rights, parties, or church does not keep today

electronic file of its members? Which of those organizations does not create a group on a social network? Aren't more and more individuals are willing and able to share their ideas on a blog? Which mobile network does not operate without processing the location data of its subscribers in order to connect a call? Which search engine can answer your request without learning about your interests? Which Internet service provider does not know which web site you are using? Which doctor, hospital, or social security service does not process your intimate data? Which clothes, mobile, or individual won't carry RFID chips in the future for one purpose or another? None.

All those devices and services process personal data relating to our fundamental rights, privacy, association, religious belief, free movement, free speech, free information, and above all to dignity and autonomy.

So the data protection and privacy principles and methods that protect us from the diverse risks of abuse referred to above, in practice protect more than privacy. They protect all of our fundamental rights.

From this assumption, on the highest level of legal norms, among the approximate number of 50 countries which have adopted so far binding data protection rules, we see these trends.

In the European Union, 13 Member States out of 27 recognize explicitly in their constitution data protection as a specific fundamental right. This is particularly true in countries which achieved democracy after the recognition of DP principles, starting with Portugal and Spain, then in the Eastern and Oriental European Countries. In the "old" democracies, constitutional courts have recognized the right by jurisprudence, in particular in Germany since 1983 and in France on several occasions either on the basis of privacy or on the basis of liberties.

On global EU level, the EU Charter of Fundamental **R**ights, which was proclaimed at the Summit of Heads of States in Nice in 2001, is the first regional/international text which establishes explicitly the data protection right as a fundamental right (article 8.1). This charter will come completely into force with the Lisbon Treaty, hopefully within some months**.** Further, this provision has been already used by the European Human Rights Court in

Strasbourg in its decisions. Interesting, the wording of the EU Charter provision includes the principle of an **independent authority, raising the policy at the constitutional level, as did the Greek constitution (article 9A) earlier and for the first time**. As a mark of its influence, it has to be noted that the Charter's provision has at its origin an initiative of the EU group of DP regulators taken in 1999 under the chairmanship of the Italian DPA.

In Switzerland, which is not a member of the EU, the constitution also recognizes the DP right.

In Canada, the highest court recognized also data protection as a fundamental right.

In other countries, we are seeing the start of the same evolution. For example, a committee for the reform of the constitution of Benin in Africa has recommended in a report made public early 2009 to constitutionalize the right to data protection. Other similar projects are underway in Latin America, in particular in Mexico. In Latin America, since the democratization that affected many countries in the late 80's and 90's, constitutional reforms have included introduction of the right to access to public information/documents. The right of access to personal data has also been recognized, under the interesting and innovative concept of "habeas data". On this basis, several Latin American Countries have developed or are currently developing DP rules.

III-2. How to achieve independence?

The EU Directive provides that the DPAs "shall act in complete independence in exercising the functions entrusted to them" (article 28.1). The implementation of the independence obligation is found in the national laws which implement the Directive. Those laws classically include these features.

III-2.1. Basic common rules

When establishing DPAs, Member States generally followed principles for independence contained in the so-called "Paris Principles" adopted by the UN in 1993 relating to the status of national institutions for the protection and the promotion of human rights:

- Appointment rules are clearly set out in the DP law, and appointments are effected by an

official act;

- A fixed term of office. (4 to 6 years depending on the Member State, possible renewable in all Member States);
- As the DPAs have more than a consultative power, when the DPA is a collegial one, there are rules for addressing conflicts of interests (i.e. declaration to the chairman of the interest of a member, and the concerned member does not take part in decisions related to that interest);
- Immunity is provided for member(s) for acts taken under the mandate.

III-2.2. Composition and modalities of designation aiming to insure qualification and independence

Regarding the composition of a DPA, two main models are observed in the EU, a collegial model and a single commissioner model. The designation of the member(s) also follows principles related to independence from government and from private interests. It basically takes into account the general constitutional organization of public institutions (Republic, constitutional Kingdom, federalism)

The collegial model

The collegial model is widespread but not the most common model. In the EU, Austria, Belgium, Bulgaria, France, Italy, Greece, Luxembourg, Netherlands, and Portugal have a collegial DPA. Outside the EU, the collegial model is found in Burkina Faso, Quebec, Mexico, Monaco and Senegal.

The pluralism and qualification of members of a collegial body depend on the appointment of members who represent diverse backgrounds and constituencies and on the ability of the members to handle human rights and technological matters. In the EU, the number of members varies from three in Luxembourg and Netherlands, to four in Italy, to over ten in Portugal and Greece, up to 17 in France (12 members of the 17 members are designated (2

each) by the following institutions, the two chambers of the Parliament, the Supreme Administrative and the Supreme Judicial Court, the Accounting Court, the Social and Economic Council, with five additional persons designated one each by the chairmen of the two parliamentary chambers and three by the government). In Belgium the Parliament selects members from those nominated by the government. The government is obliged to nominate twice as many individuals as the number of members to be selected.

In order to provide more independence under the collegial model, the chairman of the institution may be elected by the members themselves, such as in France, or designated by other means, such as by a higher institution, such as the King in Luxembourg and, outside the EU, in Morocco.

The one commissioner model

The "one commissioner" model is applied elsewhere in EU, sometimes using different procedures involving an ad hoc independent jury before the appointment is made by the government. Increasingly the designation is made by the Parliament itself. In Germany, the federal DPA was at first designated by the government, but she/he is elected now by the Parliament. In the German Lander, DPAs are also selected by provincial Parliaments.

This model, often completed by the designation of one or two deputies commissioners, typically includes procedures insuring competence and independence. The DP Supervisor and Deputy Supervisor for EU institutions are chosen by consensus by the Council of Ministers and the Parliament from a list prepared by an ad hoc independent jury set up by the European Commission after hearing from candidates responding to a public solicitation.

Particular provisions

Depending the legal administrative system, the DP law may contain the EU particular provisions aiming to help independence from outside and from inside. Such provisions indicate for example that the DPA may not receive any order and that the DP member takes

the oath of independency in a ceremony at the Constitutional Court or at the Supreme Court.

III-2.3. Funding and level of resources

In the EU, the budgets of the DPAs are transparent and permit them to have their own infrastructure and staff in order to be independent of the government . In France, for example, the DPA's budget is a specific line of the annual public budget and is voted on by the Parliament.

Decisions on expenditures are not subject to a priori approval by any other institution (which otherwise would affect its independence). Expenditures may be reviewed after the fact through the same fiscal oversight mechanisms as for any other public institution.

The level of founding for DPAs varies considerably among Member States. In particular, the French DPA's chairman fights regularly for more staff. In order to raise funds, some Member States impose a fee on the notification duty of enterprises (UK, Belgium).

III-2.4. Publicity of the DPA's work

The regular publication of an annual report by a DPA, as well as its opinions on public projects, draft bills or regulations are important functions that raise public awareness. These activities help a DPA assert its independence and demonstrate its impartiality. So does publicity for its decisions when its powers of sanction are used. The publication of the annual report is provided for explicitly in the EU Directive.

Conclusions

The necessary basic functions for effective data protection oversight and enforcement on national level and on the EU level seem to have been carefully established based on history prior to the first step of harmonization (Directive of 1995). This does not mean that all is

perfect .There are still deficiencies on one or another point in some Member States, i.e. restricted powers over secret services, several authorities for different sectors at sub national level, missing prior DPA's opinion on governmental projects or incomplete publicity over its opinions, requirement of companies' consent prior to controls on the spot… However, there is a learning process from all Member States' experience that continues to inform views of DPA functions and activities.

While the structure of DPAs in EU varies considerably according to different traditions about the organization of government in Member States, the various structures still enable DPAs to develop strategies and methods of operation that promote continuously an effective DP right at both national and EU level. Those strategies are also subject to a learning process.

Of course, efficiency depends also on available resources, which in some cases are still notably insufficient. Resource limitations affect a DPA's capacity to accompany the use of its powers with as much as possible input from and dialogue with all stakeholders, government, parliament, industry and NGOs, together with forming partnerships with education bodies and the research sector.

It is beyond the scope of this presentation to evaluate the efficiency and effectiveness of DPAs with regard to the level of the protection of the rights of individuals. On the whole, however, it is certain that in periods of high pressure on security matters, such as during the period following the 9/11 events, the DPA may be seen as the most legitimate institution to contribute to or even to initiate a debate on which freedoms should not be restricted. Most of the time, in such security situations, disproportionate measures are proposed seeking to extend the scope of security files, to collect more sensitive data, to classify individuals in new categories, to keep data for longer time, or to introduce more invasive applications, such as video surveillance. In those circumstances, the opinions of independent DPAs presented publicly are all the more important.

The rules on transfers to third countries and on applicable law preserve the DP rights of citizens, residents, and outside residents whose data are processed in the EU. But from a

general perspective of human rights and especially for efficiency, it is on the global level that the DP regulation needs much improvement as it is still lacking in consistency. Over one hundred nations have not yet adopted data protection rules, and current international instruments do not provide for proper independent monitoring or coordinated enforcement functions. The current multilateral efforts of all DPAs to improve matters will not succeed in a reasonable time without being urgently promoted by all stakeholders.

2
발 표

유럽의 독립적 정보보호 감독기구의 역사, 구조 및 기능

마리 조르쥬 (프랑스 '인포매틱스 앤 리버티즈' 컨설턴트)

먼저 IT 분야 선진국인 대한민국에서 이렇게 많은 귀한 분들과 함께 심포지엄에 참석할 수 있는 기회를 주신 것에 대해 대한민국 국가인권위원회에 감사의 말씀을 전합니다. 이 자리를 통해 제가 프랑스, 유럽 및 국제 조직에서 개인정보 및 사생활 보호 관련 활동을 수 년간 펼치면서 얻은 경험을 공유할 수 있게 되어 기쁩니다. 저는 1970년대에 사생활 보호 문제가 등장한 이후로 최근에 프랑스 자료보호 기구에서 퇴임하기 전까지 이 분야에 종사하여 왔습니다.

제가 서울을 다시 방문할 수 있도록 기회를 주신 것에 대해서도 감사드립니다. 제가 처음 서울을 방문한 것은 2002년으로 당시에는 한국정보보호진흥원(KISA)의 초청으로 국제회의에 참석하였습니다. 이 곳에 와서 한국정보보호진흥원과 비정부기구 관계자들을 다시 뵐 수 있게 되어 기쁩니다. 그 중 몇 분은 개인정보 및 사생활 보호기구(International Data Protection and Privacy Commissioners) 국제회의에서 뵙기도 하였습니다. 한국정보보호진흥원은 2004년에 그러한 국제회의에 참석할 수 있는 지위를 확보하였습니다.

유럽의 경우, 개인 정보 및 사생활 권리를 보호하기 위한 기구들은 1960년대 말과 1970년대 상반기의 정보화(전산화) 초기 단계에서 시작되었습니다. 이 감독기구들은 개인 정보 처리 과정을 통해 얻을 수 있는 부당한 권력을 제한하고 개인의 권리를 보호하기 위해 법에 의해 설립되었습니다. 이러한 정보보호기구는 국제적으로는 "Data Protection[1] Authorities (DPAs)" 또는 "Data Protection Commissioners"로 통칭되고 있습니

1) "Data Protection"은 독일에서 이 새로운 인권 분야를 지칭하기 위해 사용한 "Datenschutz"를 영어로 옮긴 것이다.

다. 프랑스의 정보보호기구는 “Commission for Informatics and Freedoms”로 불리며, 이 명칭은 프랑스 기관의 관할권이 사생활 분야에 머물지 않고 더 광범위함을 의미하며, 이는 유럽의 다른 국가들에서도 마찬가지입니다. 이에 대해서는 나중에 다시 말씀드리기로 하겠습니다.

DPA는 업무상 독립성을 필요로 합니다. 유럽뿐만 아니라 세계 모든 국가에서도 마찬가지입니다. IT의 개발과 이용은 거의 모든 인간 활동에 있어 필수적 요소이기 때문에, 지속가능한 정보보호체계를 위해서 독립성은 매우 중요합니다. 민주적 가치의 안정성을 보장하기 위해서도 정보보호권의 보전을 확보하여야 할 상관적 필요성이 있습니다. 전 세계가 부분적으로는 IT 확충을 통해 현 국제 위기로부터 회복하기 위해 안간힘을 쓰고 있는 시점에서 그 필요성은 더욱 큽니다.

도입: 역사 및 현황 개요

EU의 DPA 구조, 기능 및 독립성과 현황을 세부적으로 논하기 전에, 먼저 관련 역사와 향후 방향에 대해 간략하게 소개하기로 하겠습니다.

역사적 사실

1970년 - 독일의 헤세주(Lander of Hess)는 여러 정부 부처들의 개인정보처리를 공용 컴퓨터 센터에서 집중화한다는 계획과 관련하여 공개 논의를 거친 후에 **세계 최초로 공공부문에 대한 포괄적 정보보호법**을 채택하였습니다. 이 법은 독립적인 감독기구의 설립을 명시하고 있습니다.

1973년 - 스웨덴은 **세계 최초로 공공부문과 민간부문의 개인정보 파일에 적용되는 포괄적 정보보호법**을 채택하였습니다. 이 법에도 독립적 감독기구의 설립이 명시되어 있습니다.

1978년 - 프랑스는 포괄적 정보보호법을 채택함으로써, **세계 최초로 독립적이고, 공조적이며, 다원적인 DPA**를 설립하였습니다. 이 법은 공공부문에서 비용효율적 관리 방안의 하나로 기존의 사회보장번호를 일생동안 부여되는 고유한 식별체계로 변경한다는 내

용의 SAFARI 프로젝트에 대해 대대적인 반대 여론이 형성되면서 제정되었습니다. 의회 승인 과정에서 DPA를 행정부 통제하에 두려는 행정부의 의도에 대해 양원의 여당과 야당 의원들이 강하게 반발하면서 진통을 겪기도 하였습니다. 또한, 프랑스 의회는 교묘한 법 회피를 막기 위해 세계 최초로 **수기 파일**에 대해서도 적용된다는 조항을 추가하였습니다.

1979년 - 독일의 DPA 주최로 본에서 **최초의 DPA 국제회의**가 개최되었습니다. 이는 국가별 DPA간의 국제 협력이 시작되고 국제 무대에서 그들의 영향력이 확대되는 계기가 되었습니다.

1981년 - 유럽이사회는 EU 회원국간에 자유로운 정보 이동을 보장하면서 동시에 정보 보호권을 보장하기 위해 **구속력 있는 협약**(No. 108[2])을 채택하였습니다. 이 협약의 필요성은 최초의 국내법의 채택에 맞먹는 것입니다. 이 협약이 채택되기 수 개월전에, 구속력 있는 기제의 채택을 지지하지 않았던 미국 대표단은 대신 그에 상응하는 OCED 차원에서의 조치를 추진하였으며 그 결과 OCED는 1980년 후반에 **구속력이 없는 가이드라인**[3]을 채택하게 되었습니다. 이 기제에 명시된 원칙들은 서로 유사하며 **1970년대 초 미국에서 마련된 '공정정보원칙(Fair Information Principles)**'과도 유사합니다. 그러나, 제 3국가에게도 열려 있는 **유럽이사회 협약**이야말로 차별을 방지하기 위해 **소위 민감한 정보의 처리에 대한 규정을 강화한 최초의 구속력 있는 국제 기제**라 할 수 있습니다. 이 기제들 중 어느 것도 DPA의 설치를 의무화하고 있지는 않습니다. 유럽이사회 협약은 이와 관련하여 추후에 개정된 바 있습니다.

1991년 - 유럽이사회 협약과 OCED 가이드라인의 초안 작성에 참여하였던 - 그리고 이전에는 프랑스 DPA 관련 업무의 초대 책임자이기도 했던 - 한 재판관의 보고서를 기초로 하여, **유엔 총회는 민간 및 공공부문을 모두 포괄하는 최초의 범세계적인 "전산화된 개인 파일의 규제를 위한 가이드라인(Guidelines for the regulation of computerized personal files)"**(결의 45/95, 1991년 12월 14일)을 만장일치로 채택하였습니다. 이 가이드라인은 민감한 정보의 범위를 포함하여, OCED 가이드라인 및 유럽이사회 협약 108호와

2) 개인정보의 자동처리와 관련하여 개인의 보호를 위한 협약 (협약 108호, 1981년 1월 28일 채택)
3) 사생활보호 및 개인정보의 국경간 이동에 관한 OECD 가이드라인 (OCED Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)

일맥상통합니다. 이 유엔 가이드라인은 독립 DPA에 관한 조항을 담고 있는 최초의 국제 기준으로, 감독 및 제재에 관한 8항에서 "모든 국내법은, 자국의 법제에 의거하여, 상기 열거된 원칙들의 준수를 감독할 책임 기관을 지정하여야 한다. 해당 기관은 공평성, 정보 처리 및 구축을 담당하는 개인 또는 기관에 대한 독립성, 기술적 능력을 보장할 수 있어야 한다. 상술한 원칙의 이행을 명시하고 있는 국내법 조항을 위반한 경우, 적합한 개별 구제와 함께 형사상 또는 기타 처벌이 이루어져야 한다"고 명시하고 있습니다. 그러나, 이 유엔 가이드라인은 구속력을 지니고 있지 않습니다.

1995년 - 1989년 베를린에서 개최된 개인정보보호기구 국제회의 기간 중에 독일 개인정보보호기구의 발의와 프랑스 개인정보보호기구의 지지에 힘입어, 유럽집행위원회는 국내법 조정을 위한 **입법지침**을 제안하였으며 이 지침은 **2005년 10월 25일에 유럽의회와 유럽이사회에서 채택**되었습니다.[4] 이 지침은 공공 및 민간부문에서 법이 적용되는 모든 분야에서 이루어지는 전산 및 수기 정보처리를 포괄하고 있습니다. 이 지침은 유럽이사회 협약에 바탕을 두고 있으며, 유럽 공동시장에서 국내법들의 조화를 주된 목적으로 합니다. 국제 차원에서 보면, 이 지침은 **의무적인 국내 독립 DPA의 설치와 국가 DPA간 협력을 명시한 최초의 구속력 있는 지역 기제**입니다. 또한, **EU 영토 외에서의 정보 이동과 관련하여서도 제3국에서의 적절한 보호 또는 적어도 외국인 정보 입수자의 충분한 보호 보장 제공을 요구하는 구속력 있는 조항**을 담고 있습니다. **국가간 정보 처리의 조사에 대한 정보 교류도 명시하고 있습니다. 또한, 이 지침에는 국가 DPA와 EU 기구 DPA를 구성원으로 하는 지역별 기구의 설립도 최초로 명시되어 있습니다.**

2003년 - 유럽이사회는 EU 비회원국들도 다수 비준한 바 있는 사이버범죄 협약을 채택한 지 2년 후에 DPA의 설치를 의무화하고 제3국으로의 정보 이동과 관련한 유사 조항을 마련하기 위해 **협약 108호**의 의정서를 채택하였습니다. 동 협약은 1981년 이후로 제3국에게도 개방되어 있지만, 아직까지 이 협약에 비준한 제3국은 없습니다.

2001년~2009년 - 파리에서 개최된 **제22차 DPA 국제회의**에서는, **DPA가 적법한 국제결의를 채택할 수 있도록** 하기 위해 **DPA의 인증에 관한 규정**이 채택되었습니다. 2005년 WSIS (정보사회세계정상회의) 개최 전날에 열린 제27차 회의에서는 **특히 유엔과 유럽이**

4) 1995년 10월 24일에 채택된, 개인정보의 처리와 관련한 개인의 보호 및 그러한 정보의 자유로운 이동에 관한 유럽의회 및 이사회 지침 95/46.EC (Official Journal L 281, 23/11/1995 p.0031-0050)

사회에게 범세계적 차원의 구속력 있는 국제 기제 수립을 촉구하는 결의문을 채택하였습니다. 국제 차원에서의 정보 처리는 지속적으로 확대되고 있는데도 불구하고 전지구적 단계의 정보보호활동이 미흡함을 고려하여, **11월에 마드리드에서 개최되는 31차 DPA 국제회의에서는 법집행을 위한 국가 DPA간의 국제적 협력을 요구하는 국내법 조항을 포함하여 더욱 보완된 국제최저기준 체계를 권고할 예정입니다.**

국제 현황 개요

지금까지 전 세계에서 정보보호법(DP 법)을 채택한 국가는 50개국이 넘습니다. 그 외의 상당수 국가들도 DP 입법을 검토중에 있습니다.

오늘날 DP 법 또는 법안이 DPA에 관하여 명시하고 있지 않은 경우는 드물며, 그러한 경우라도 DPA의 필요성은 공공 논의 및 의회에서 반복적으로 거론되고 있습니다.

또한, DPA가 공공부문 및 민간부문 모두에 대한 감독 기능을 갖고 있지 않은 경우도 일반적이지 않습니다. 드물게, 일부 기관들은 민간부문의 일부에 대해서만 정보보호 권한을 지니고 있습니다. 예를 들어, 미국에서는 연방통상위원회(Federal Trade Commission)은 인권보다는 소비자 권리와 관련된 법에 근거하여 민간부문의 일부에 대해서만 제한된 권한을 지니고 있습니다. 미국에서는 1974년부터 독립적인 DPA의 수립에 대한 주장이 의회에서 간헐적으로 제기되고 있지만 아직까지는 성과를 거두지 못하고 있는 실정입니다.[5] 대신, 특정 연방 정부기관내에서 (독립성은 결여된) 내부적 감독 체제가 마련되거나 민간 기업에서 자발적 사생활보호 담당관제도가 운영되는 경향을 보이고 있습니다.

EU의 경우, 1995년의 합동 지침 채택과 EU 회원국의 지침 이행을 통해, 27개 회원국 전부, 유럽경제지역(EEA) 회원국 3개국, 가입 후보국 2개국에서 독립적 DPA가 수립되는 성과가 있었습니다. 이 기관들은 국내적으로는 민간 및 공공부문에 대해 권한을 지니며 EU 밖에서의 정보 이동에 대해서도 권한이 있습니다. 또한, 집행권을 지니며, 유럽 차원에서 영향력 있는 자문단에 참여하고 있습니다.

기존의 불완전한 국제 DP 규정 체제는, 국제기준에 의거한 국내법 채택과 국제 차원

5) Robert Gellman, Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions, VI Software Law Journal 199 (1993)., http://bobgellman.com/rg-docs/rg-softwarelj.pdf; A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board, 54 Hastings Law Journal 1183 (2003)., http://bobgellman.com/rg-docs/Gellman-Hastings-03.pdf.

에서 더욱 공조적인 규제 및 집행 매커니즘의 수립을 촉진하기 위한 목적으로 개별 DPA와 DPA 국제회의에서 주창하는 새로운 구상안에서 혁신의 대상이 되고 있습니다.

***

저는 이 글의 주제와 관련하여, 유럽과 제가 활동한 경험이 있는 기타 국가들, 특히, 아프리카와 남아메리카 국가들의 현황을 기술하기 위해, 다음과 같은 몇 가지 질문을 던지고 이에 답하는 형식을 취하고자 합니다.

- 왜 DPA여야 하는가? 국제적 차원에서의 경우를 포함하여, DPA의 필수 기능은 무엇인가?
- 왜 DPA는 공공과 민간부문 모두에 대해 권한을 지녀야 하는가? 왜 DPA는 기타 인권 관련 권한을 지닐 필요가 있으며, 어떠한 권한을 지녀야 하는가?
- 왜 DPA는 독립적이어야 하며, 어떻게 독립성을 확보할 수 있는가?

I- 왜 DPA여야 하는가? DPA의 필수적 기능은 무엇인가?

I-1. 정보처리 리스크 및 해당 DP 원칙의 일반적 성격: 균형 촉진 및 이행 보장의 필요성

제3자가 보유하고 있는 디지털화된 개인정보가 해당 개인에게 어떠한 일반적 위험을 내포하고 있는지는 매우 잘 알려져 있습니다. 즉, 정보는 쉽게 사본으로 작성되고, 타인에게 전달될 수 있으며, 소실 또는 파기되고, 매우 낮은 비용으로 수 년간 이용되거나, 수집 당시 목적 외로 비밀리에 또는 동의 없이 재사용되며, 개인 또는 통계적 프로파일을 기초로 하는 자동 결정에 사용됩니다.

이미 이러한 위험을 70년대 초반에 밝혀낸 유럽과 미주 지역의 전문가들은 개인정보처리 담당자의 세부적 의무를 규명하고 개인의 권리를 명시하는 일련의 기본 원칙을 작성하였습니다. EU에서 이행되고 있는, 여타 국제 문서들보다 더 세부적인 이 원칙들은

다음을 주요 내용으로 하고 있습니다.

- 정보 주체에 대한 통보 없이 개인정보 관리자(정보처리를 지휘하는 자)의 권한을 부당하게 강화할 수 있는 정보 활동을 금지하는, 책임성(responsibility)과 투명성(transparency) 원칙
- 정보 주체의 인지 또는 동의(반대 또는 동의할 권리) 없이 다른 목적으로 개인정보를 남용, 재사용 또는 매칭하는 것을 금지하는, 정당한 목적(legitimate purpose)과 양립불가 목적(incompatible purpose) 원칙
- 불필요한 정보 수집과 필요성 소멸 후 정보 보유를 금지하는, 비례성(proportionality) 또는 최소화(minimization) 원칙
- "민감한" 정보를 다루는 경우에 관한 보강된 규정
- 개인정보가 제3국으로 이동되는 경우 제3국에서 주어지는 보호 수준의 적정성
- 보안(security) 원칙
- 개인이 자신의 정보와 관련하여 통보 받고, 자신의 정보에 접근하며, 필요한 경우 정보를 수정, 완성 또는 제한할 수 있으며, 정보의 출처에 대해 알고, 정당한 근거에 의한 처리에 대해서도 반대할 수 있으며, 보호 장치 없는 프로파일링에 의해 이루어지는 자동화 결정의 대상이 되지 않을 권리
- 중대한 특정 공익에 따른 예외(derogations)는, 필요한 경우, 민주 사회에서, 공개적이고 명료하며, 입법부가 정한 헌법적 기준에 근거하여 채택될 수 있다.

이러한 원칙은 특정한 기술이나 맥락에 한정되지 않고 일반적 성격을 특징으로 합니다. 이와 동시에, 공공 또는 민간부문에 관계없이 정보 처리를 담당하는 이들의 이해는 위 원칙들과 상충할 가능성이 큽니다. 이러한 상황에서 불확실성과 유혹이 발생하게 됩니다.

따라서, 공정하고, 자격과 경험을 갖춘 이들이 외부 감독을 통해 적절한 균형(즉, 정당한 목적은? 균형 잡힌 대응은?)을 맞출 수 있도록 지원할 필요가 있습니다. 게다가, 정보처리량과 관련 개인의 수를 고려하면, 이러한 필요는 의회나 사법부 기관이 제공할 수 있는 것보다 더 신속하고 세부적인 방법으로 충족되어야 할 것입니다.

EU는 효율성 보장을 목적으로 주로 DPA에 의해 운영되는 다차원적 체제(multi-dimensional system)에 의존하는 방법을 택하여 왔습니다. 이 체제는 1995년 DP 지침의 해당 조항을 참조하여 다음과 같은 주요 요소들을 포함하고 있습니다.

- 해당 개인과 관련하여 보장되는 투명성 (정보수집 당시 통보) 외에도 DPA 통고를 통해 모든 정보처리의 투명성 확보 (규정 또는 사생활 보호관(Privacy Officer) 제도의 운영에 따른 예외 인정) (제18조)
- 구체적인 인권 위험을 안고 있는 공공 및 민간부문의 프로젝트에 대한 DPA (견제와 균형) 또는 의회의 사전 의견 (제20조, 28조)
- 법 이행을 보장하기 위해 업종별 대표들이 작성한 행동규범에 대한 DPA의 검토 (제27조)
- DPA의 조사권과, 국가별 선택 여부에 따른, DPA의 제재 부과 및 구제 제공권. 유럽의 DPA는 진정건 심리, 조사 실시, 가처분 명령의 권한이 있으며 비공식 조정에 의한 사건 해결이 가능하고 (진정건 90% 이상의 경우), 국가별 선택에 따라 차이가 있으나, 위반건에 대해 제제 및 구제를 실시하거나 (가령, 프랑스, 그리스, 이탈리아, 네덜란드, 스페인의 경우에는 DPA가 과징금 부과할 수 있으며 이탈리아 DPA는 구제 조치를 취할 수 있다) 법원에 제소할 수 있다.
- 개인은 법원에 진정할 수 있는 가능성을 지닌다. (제22-24조, 28조)
- 정보처리에 관련된 법안, 특히, DP 원칙을 유보하기 위한 목적의 법안과 정부 규정에 관하여 의견을 제기할 수 있는 DPA의 권한

28조에 명시된 바와 같이 DPA가 내린 모든 결정은 법원에 항소할 수 있습니다. (프랑스의 경우에는 대법원을 통해)

그렇다고 해서 EU의 상황이 이미 이상적인 수준에 있다는 말은 아닙니다. 회원국들은 지침을 이행하는 과정에서, 지나치게 관료적인 체제를 채택했거나 또는 그 반대로 어떠한 영역에서 DPA에게 충분히 효과적인 권한을 부여하지 못하고 있기도 합니다.

그러나, DPA에 주어진 다양한 권한과 언론의 자유를 통해 DPA는 공공 및 민간부문에서 DP 권리에 영향을 미치는 어떠한 정책에 대해서도 공개적으로 비판할 수 있습니다.

I-2. 급속한 IT 혁신: DP 문화의 활성화, 모니터링, 특정 권고, 기술 개발 유도, 행정부와 의회에 관련 추가 규정 또는 정책의 필요성을 인지시켜야 할 필요성

새로운 유형의 IT 혁신은 때때로 새로운 주체들에 의해 선도되거나, 새로운 목적을 위해 고안되며, 특정 집단에게 이롭게 또는 불리하게 새로운 부문에 또는 새로운 기능으로 활용됩니다. 예를 들자면,

통화 연결을 위해 기술적으로 수집되는 이동 위치 추적 정보는, 가족 또는 직원의 위치를 파악하려는 새로운 목적 및/또는 상업적 목적으로 통신업체에 의해 제공되고 있습니다.

폐쇄 집단을 위해 고안된 사회적 네트워크도 갑자기 디폴트 기능, 적절 기능 및 사생활 보호적 기능도 없이 모든 사람에게 제공되기에 이르렀습니다.

경찰 업무를 위해 사용된 바이오메트릭스 시스템을 기반으로 하는 시스템이, 근무 시간 기록이라는 새로운 용도에 이용되고 있습니다.

원래는 물품 운반대의 분배를 관리하기 위해 고안되었던 라디오 주파수 식별(RFID) 기술은 현재 적정한 보호 장치 없이 국경 통제, 여권 및 유사 업무에 의무적으로 사용되고 있습니다.

이러한 신기술이 사용된 지 얼마 되지 않았기 때문에, 해당 개인이나 여론 지도자들이 그러한 사용 현황에 대해 모를 수도 있습니다. 새로운 용도를 통해 이익을 얻고자 하는 사람들은 그러한 기술이 가져올 수 있는 사회적 위험과 자유 침해 및 기타 결과에 주목하지 않으며, DP 원칙을 적절하게 적용하지 않을 수 있습니다.

좀 더 일반적으로 말해 IT 신기술은 빠른 성장, 새로운 기능, 투명성 결여, 다른 모든 종류의 대상과의 통합, 침해적 활동 (가령, 인터넷 프로토콜 주소의 수집이나 이용, 비디오 감시, 바이오메트릭스, RFID, DNA), 응용기술 이용 속도의 증가, 출생 전부터 사망 후까지의 더욱 일상적인 활동과의 연계 등을 포함해 다진화적(multi-evolutionary)이고 확대되는 속성이 있으며 사회구조에 막대한 영향을 미칩니다. 따라서 정보보호 기능을 갖춘 상시적 체제가 요구되며 EU에서는 독립적 개인정보보호기구들이 이러한 역할을 맡

고 있습니다. 예를 들어, 개인정보보호기구는,

- 정보보호에 대한 인식을 고취시키고, 라디오, TV, 인터넷, 회의, 전문가 포럼 (가령, 프랑스에서는 정보보호의 과정 소개 활동에 교육부와 대학 총장들이 참여하고 있음) 등에 의한 커뮤니케이션을 이용함으로써 정보보호 문화를 증진할 수 있습니다.
- IT 동향을 모니터링하고, 향후 이용을 예측하며, 연구 활동 및 기술 표준화 기구에 영향력을 행사할 수 있습니다.
- 조언을 제공할 수 있습니다.
- 관련 직종 및 관계자 대표들과 협의를 거쳐 경험에 근거한 권고를 채택, 배포할 수 있습니다. 예를 들어, 프랑스 DPA는 웹 포럼에서의 언론의 자유를 보장하기 위한 방법에 대해 권고하였으며 (저자의 이름을 공개할 필요는 없으나, 나찌 활동을 옹호하는 광고와 같이 공개된 글이 헌법상 제약을 위반하는 내용이 되지 않도록 중재자를 정해야 할 필요는 있음), 또한 지문을 사용하는 바이오메트릭스 시스템은 보안상 위험이 큰 경우에 한하여 사용을 허용하고 직원의 근로시간 기록에는 사용하지 못하도록 하는 등, 바이오메트릭스의 균형 잡힌 이용 방법에 대해 권고한 바 있습니다.
- 그러한 권고 사항의 이행을 모니터링 하고, 조언대로 이루어지지 않은 경우에는 정치적 단계에서 (행정부와 의회에) 구속력 있는 추가 관련 규정의 필요성을 경고할 수 있습니다. (프랑스의 경우, 바이오메트릭스 시스템이 자유의 침해 위험이 있어 권고만으로는 충분치 않다고 간주되어, 대부분의 응용 기술이 DPA의 사전 승인을 받도록 되어 있음)

이러한 기능을 수행하기 위해서는 많은 비용과 시간이 요구되며, 그렇기 때문에 EU 차원에서 DPA들 간의 협력이 정책 보완에 가장 효과적인 것으로 생각됩니다.

이 모든 기능들은 향후 정보처리에 널리 사용될 것으로 예상되고 있는 나노기술을 감안하면 그 중요성이 더욱 커집니다.

I-3. 보완적인 법적 도구와 신기능: “개인정보보호관 (사생활 보호관) 제도”와 인증제

개인정보처리활동이 폭발적으로 증가하는 상황에서 효율성을 보장하기 위해 EU내에서는 두 가지 주요 도구의 추가 이행이 고려되고 있습니다. 바로, 개인정보를 보유하고 있는 조직내에서 실시하는 “사생활 보호관(privacy officer) 제도”와, 인증제(certification)입니다.

개인정보보호관(Personal data protection official (privacy officer))

상당수의 개인정보처리 활동이 전문적으로 수행되는 경우에는 (80% 이상) 특정 위험의 문제가 없다는 점을 감안하여, EU 정보보호지침(EU Data Protection Directive)은 회원국이 DPA 통지 의무의 두 가지 예외 중에서 선택할 수 있도록 하고 있습니다 (제18조). 첫 번째는, 개인정보처리를 책임지고 있는 정보 관리자가 개인정보보호관(프랑스에서는 “correspondent for informatics and freedoms”으로 불림)을 지정하는 것으로, 이는 독일에서 유래된 방식입니다. 두 번째는 허용가능한 주요 정보처리 특징(목적, 대상자, 처리정보목록, 입수자)을 명시한, DPA가 채택한 규정에 근거하여 예외로 할 수 있으며, 이는 스웨덴, 프랑스, 네덜란드에서 채택하였던 방식입니다.

일부 회원국은 EU DP 지침의 이행을 위해 사생활 보호관 제도를 의무적으로 또는 자발적으로 실시하도록 정한 바 있습니다(가령, 네덜란드와 프랑스). 이러한 접근 방법이 향후 EU에서 더욱 보편화될 것으로 보입니다.

인증제(Certification)

새로운 기능, 프로토콜, 상품과 점점 더 많은 정보처리 서비스를 제공하는 기술 - 이 중 상당부분이 이미 많은 사람들에게 일상 생활의 필수 요소임 - 로 인해 EU내에서는 인증제의 필요성이 제기되어 왔습니다.

독일의 슐레스비히 홀슈타인(Schleswig Holstein)주는 사전 통제의 미비함을 보완하기 위해 DP 인증제 절차를 실시한 최초의 사례입니다. DPA가 요청에 따라 인증서를 제공하며 그 비용은 인증서 수요측이 부담하게 됩니다. 해당 상품 또는 서비스는 검증된 전

문가 명단에서 선정된 독립 전문가들이 사전에 평가합니다.

EU 인증제에 관한 유럽내 연구 프로젝트가 현재 슐레스비히 홀슈타인주의 DPA의 주도하에 진행중이며, 프랑스와 마드리드 DPA가 참여하고 있습니다.

프랑스의 DP 관련법에는 이미 그러한 방식이 명시되어 있어서 DPA에게 인증서 발부 권한이 주어져 있습니다. 그러나, 지금까지 그러한 권한이 시행된 바는 없습니다.

EU 회원국이 아닌 유럽국가로서는, 스위스의 DPA가 인증서를 발부하고 있습니다. EU 회원국의 DPA 중 상당수가 향후 이러한 방식을 검토해야 할 필요성을 제기하고 있는 상황입니다.

I-4. 국제적 협력 기능

IT 신기술의 등장(바이오메트릭스 캡터(biometrics captor)와 같이, 개인정보처리를 위한, 또는 개인정보를 이용하는 IT 상품의 생산 및 유통 국제화)과 함께 개인정보처리 및 관련 서비스 초국적 성격이 점점 커지면서 (가령, 인터넷 웹사이트, 다양한 외주 업무, 유비쿼터스 전산, 타국 기관에 자료 전송 등), 국가별 DPA 기능의 상당수가 국제적 차원에서의 협력을 필요로 하고 있습니다.

지금까지는, EU 지역에서만 이러한 기능들이 EU 차원에서 제도화되어 있으며, 독립적 감독기구를 기반으로 하는 전지구적 차원의 국제 협력은 이루어지지 않고 있습니다. 그러나, DPA들은 1979년 이후로 자발적으로 자체 수단을 동원하여 국제 차원에서 더욱 더 영향력 있는 네트워크를 구축해 오고 있습니다. 그렇다고 해도, DPA가 공동의 사건 조사에 관한 자료를 교환함으로써 상호 협력하는 일은, 당사자에 대한 적절한 민주적 보장과 함께, DPA에게 그러한 자료 교환 권한을 부여하는 상호 (그리고, 더 효율적인 것은, 다자간) 협약이 체결되지 않는다면 불가능할 것입니다.

I-4.1. EU 차원에서의 지역 DPA 기능과 방법

국가 단계에서 집행되는 기능인 청구 심리와 조사에 있어, DPA는 초국적 정보처리 관련 법규에 따라 권한을 지니는 타 DPA를 위해 자국 영토내에서의 권한을 행사함으로써

협력하여야 합니다(1995년 일반지침 제28.6조).

IT 모니터링과 DP 규제와 관련하여 국내에서 지니는 역량 외에, DPA는 "개인정보처리와 관련하여 개인의 보호에 관한 실무단(Working Party on the Protection of Individuals with regard to the Processing of Personal Data)"이라는 명칭으로 EU 차원에서 조직한 네트워크 내에서 일정한 권한을 지닙니다. EU 지침 제29조에 의해 수립된 이 실무단(일반적으로는 29조 실무단 또는 WP29라고 불림)은 필요한 권고를 발의하거나 채택하고 유럽 집행위원회를 위해 다음과 같은 협의적 성격의 업무를 수행할 수 있는 광범위한 권한을 가집니다(제30조).

- 지침 조항이 일관되게 이행되도록 기여.
- 유럽 공동체내에서와 제3국에서의 보호 수준에 관한 의견을 제시. 제29조 실무단은 비회원국이 그곳의 정보 입수자에게 개인정보가 제공될 수 있도록 적절한 수준의 보호를 보장하고 있는지 여부에 대하여 의견을 제시하고 있습니다. 유럽 집행위원회는 제3국이 적절한 수준의 보호를 보장하고 있지 않다고 결정할 수 있는 권한이 있습니다(제25조).

  적정성에 관한 일반 정책을 수립하기 위하여, 이 실무단은 적정성 평가 방법 및 지침에서 명시한 면제 조항의 해석과 인정 방법에 관한 일련의 일관되고, 유연한 세부 보고서를 작성하였습니다. 특히, 비적정 국가에 위치한 입수자에 대한 정보 제공은 계약서에 충분한 보호가 명시되어 있거나 EU DPA 집행권을 인정하는 소위 "구속력 있는 사칙(binding corporate rules)"이 존재하는 경우에 허용될 수 있습니다. 이에 관한 WP29 보고서는 이후 유럽 집행위원회 평가와 국가별 결정에 있어 근간이 되었습니다.
- EU 지침의 개정안, 개인정보처리와 관련하여 자연인의 권리와 자유를 보호하기 위한 추가 세부적 대책, 이러한 권리와 자유에 영향을 미치는 기타 EU 대책안에 관하여 자문 제공
- EU 차원에서 작성된 행동규범에 대한 의견 제시

실무단이 채택한 150건이 넘는 실무작업문서, 견해서, 권고서 및 해석적 성격의 실무보고서는 모두 공개되어 있습니다. 가장 영향력이 큰 실무보고서(WP papers) 일부는 개

인정보의 개념, 그리고 DP 원칙을 인터넷, 전자정부(e-government), 고용정보처리, 비디오 감시, RFID, 바이오메트릭스, 검색 엔진 및 사회적 네트워크에 적용하는 내용을 다루고 있습니다.

(http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm 참조)

실무단은 보고서를 채택할 때, 당사자 대표의 의견을 수렴하고 초안에 대해 온라인 협의를 거칩니다.

실무단은 의장과 부의장을 선출하여, 연간 4차례 이상의 회의를 갖고, 연간 업무 프로그램을 기획하며, 필요한 경우 소그룹을 구성합니다. 정보보호를 담당한 유럽 집행위원회 부서는 자체 사무국을 운영하고 있습니다.

또한, 실무단은 유럽 집행위원회의 초청으로 정책안 수립을 위한 그룹에 참여하고 있습니다. 예를 들어, 실무단은 RFID에 관한 2005년 보고서를 발간한 후에, 2007년과 2008년에 해당 그룹에 참여하여 RFID에 관한 권고를 작성하였으며, 이 권고는 유럽 집행위원회가 2009년 5월 12일에 채택한 바 있습니다 (제공자에 의한 RFID 이용에 대해 사전 사생활 보호 평가를 각국 DPA가 실시하며, 소비자가 RFID 장치(tag)의 사용을 동의하지 않는 경우에는 판매자가 판매시점에 그 장치를 해제하고, EU 표준화 기구는 RFID 장치와 판독기(reader)의 투명성을 위한 로고스를 개발하도록 촉구하는 내용[6]).

이 외에도, 실무단은 유럽의회의 자문단으로서 역할도 점차 커지고 있습니다. 가령,실무단은 미국과 기타 국가들이 요청하고 있는 항공 예약 시스템에 사용된 승객명단기록(PNR)의 공개와 관련하여 자문을 제공하였습니다. 이와 관련하여, 벨기에의 법학 교수인 Y. Poullet와 S. Gurtwirth이 EU내 DP 운용에 있어 제29조 실무단의 역할에 관하여 저술한 논문[7]을 참조하시기 바랍니다.

I-4.2 DP 및 사생활 보호기관(Privacy Commissioners) 국제회의에서의 협력

DPA는 관련 제도의 역사가 짧은 데다가 국내에서 직면한 문제점들이 서로 유사하기

6) http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

7) The contribution of Article 29 Working Party to the construction of a harmonizing European data protection system ; an illustration of « reflexive governance », Prof Yves POULLET, director of the Crid, Faculty of Law, FUNDP, Namur, and Prof.S.GUTWIRTH, Law, Science, Technology and Spciety, Faculty of Law and Criminology, Vrije Universiteit Bruseels, Belgium

때문에, 양자간, 그리고, 이미 1979년부터, 다자간 차원에서 견해를 교류하려는 기회를 모색하여 왔습니다. 이제는 연례행사가 된 DPA 국제회의는, 독일 DPA의 주최로 독일 본에서 최초로 개최되었습니다.

국내외적으로 불안한 지위에 있는 DPA에 대해 지속적인 지원이 필요하기도 하였고, 그와 함께, 정보, 서비스 및 산업 규정의 초국적 이동이 점증하는 데 대해 개인정보처리 관련 국제기구들(ICAO, ISO 등)이 공동의 입장을 마련하여야 할 필요성도 커지면서, DPA는 국제적 차원에서 공동의 관심사에 관한 결의문을 채택하기에 이르렀습니다. 한 예로, 가장 최근인 2008년 프랑스 스트라스부르그에서 독일과 프랑스 DPA의 주최로 열린 국제회의에서 온라인 아동보호, 사회적 네트워크 결성, 사생활 보호와 개인정보보호에 관한 국제기준 수립에 관하여 채택된 결의문을 들 수 있습니다(www.privacyconference2008.org).

결의문 채택은 DPA가 결의문 초안 도입 방식에 관한 규칙(최소 회의 1개월 전에 3개 이상 DPA의 지지를 필요로 함)과 2001년 프랑스 회의에 참여 및 의결권 행사에 관한 규정(보고서를 작성하고 총회 결의문 초안을 작성하는 인증위원회의 승인을 필요로 함)을 2000년 (이탈리아에서) 승인한 이후로 가능하게 되었습니다. DPA는 법에 의해 독립적인 지위를 지닌 국가 DPA로서, 감독하는 DP 권리가 OECD, UN, COE 또는 EU의 DP 기준에 명시된 국제 원칙에 부합되고, 자국 헌법에 의해서만 권한이 제한되며, 광범위한 활동에 대해 관할권을 지니는 경우에 의결권을 갖게 됩니다. 미인증 DPA는 옵서버의 지위가 주어지며, 국가하위단계의 DPA(subnational DPA)는 토의에 참가할 수 있습니다.

그러나 이 국제회의는 아직까지 법적 지위나 상설 사무국을 갖고 있지 않습니다. 사무국은 마지막으로 국제회의를 주관한 DPA가 운영합니다. 결의에 의해 설치된 소위원회는, 상설 웹사이트(미설치)의 설치 방법이나 DP 문제를 다루는 국제기구로서 인정 획득(ONU, CoE, OECD, ISO 등과 같이)과 같은 공통의 관심사에 관하여 지속적인 활동을 펼치고 있습니다. (www.privacyconference2008.org 참조).

I-4.3. 동일 언어를 사용하는 국가들에서 DP법 활성화를 위해 EU DPA들이 취한 특별한 방안: 성공적 결과

2005년 튀니스에서의 세계정보사회정상회의(WSIS)가 개최된 이후로, DPA 국제회의

(2005년 스위스 몽트뢰)는 각국 정부, UN 및 유럽이사회에 전지구적 규모의 국제 회의를 통해 전지구적 단계에서 정보보호 규정을 추진할 것을 촉구하여 왔지만, 지금까지 이렇다 할 성과를 거두지 못했습니다. UN 국제법위원회도 이와 관련하여 보고관을 지정하지 않았습니다. 그러다가, 작년에 유럽이사회(CoE)가 협약 제108호와 부속 의정서를 촉진하기 위해 개별국가들과 접촉할 의사가 있다고 발표하였습니다. 국제 기제를 마련하거나 유럽이사회 협약을 촉진하기 위한 절차는 전지구적 차원에서의 효율성을 증대시킬 것이며 아직까지 DP법제가 없는 국가들에게는 그러한 법제를 신설하도록 인센티브를 제공하게 될 것입니다.

DPA가 동일 언어를 사용하는 국가들에 대해 직접적인 방법을 실시함으로써 성과를 거두고 있습니다. 스페인어, 포르투갈어, 프랑스어를 사용하는 국가의 DPA가 아직 DPA가 설치되지 않은 동일 언어 사용 국가들과 경험을 공유함으로써 정보보호에 대한 인식을 고취시키고 있습니다. 멕시코, 우르과이, 마카오, 모로코, 부르키나파소, 세네갈, 베냉에 대해서도 성공적인 협력 사업이 추진되어 왔습니다. 이 국가들의 DPA의 제안에 따라, 현재 해당 언어의 국제기구들이 국가원수 정상회의에서 DP권과 DPA간 협력 증진을 지지하는 선언에 뒤이어 원조를 제공하고 있습니다. 특히, DP 관련 국제회의와 지역회의를 지원하는 프랑스어 사용 국제기구인 OIF(Organisation Internationale de la Francophonie)는 2009년 11월에는 하노이에서 IT와 관련법, 특히, DP권과 정보의 자유에 관하여 열리는 지역회의를 주최할 예정입니다. 이 회의는 프랑스어 사용 DPA 협회의 지원으로 Maison du Droit가 주관하며, OIF 회원국 및 옵저버 국가 4개국(캄보디아, 라오스, 타일랜드, 베트남)의 IT 및 관련법 전문가와 각계 대표들(정부, 의회, 사법부, 업계, 민간)이 참여합니다.

II- 왜 민간과 공공부문 모두에 대한 DPA가 필요한가? 왜 DPA 감독기능과 기타 인권 감독기능들을 통합해야 하는가? 그리고, 어떠한 기능들이 이에 해당하는가?

여러 가지 이유에서 공공부문과 민간부문 모두에 대해 권한을 지닌 DPA가 강력하게 요구되고 있는데, 국민의 이익을 위해 더욱 일관된 규정, 기타 인권 활동과의 연계 강화,

독립적인 DP 권한을 수행하는 데 있어 효율성 증대 등의 필요성을 충족시킬 수 있기 때문입니다.

II-1. 왜 민간과 공공부문 모두에 대한 DPA가 필요한가? - 규정의 일관성과 개인권의 보호를 위해

동일한 기술 사용

공공 및 민간부문은 서로 다른 목표를 추구하고 활동을 전개하는 방식도 다르지만, 사용하는 기술은 동일합니다. 한 부문에서의 핵심 기술이 이후에 다른 부문에서 사용될 수 있습니다. 예를 들어, 처음 군사 부문에서 시작되었던 컴퓨터가 정부와 민간부문에까지 확산되었습니다. 인터넷도 군대에서 시작되어, 국제 연구활동에, 그리고 더 나중에는 국제 상거래에 이용되었습니다. RFID의 경우에는 주로 민간부문에서 시작되었다가 지금은 공공부문에도 사용되고 있습니다.

동일한 업무/IT 응용기술

교육과 보건부문에서는 해당 단체가 공공이든 민간이든 관계없이 동일한 핵심 업무가 전개되고 있습니다. 공립병원은 사설 의료진들과 디지털 시설을 공유할 수 있습니다. 공공정책에 의해 구축된 진료기록 네트워크 시스템은 민간 기업이 운영할 수 있으며 공공 또는 민간 시설에서 근무하는 의료 전문가들을 지원할 수 있습니다. 마찬가지로, 공공 및 민간부문은 동일한 기술을 사용하고 동일한 DP 문제가 제기되는 인적자원관리 시스템을 운영하고 있습니다.

양 부문에서 DP 보증이 동일하지 않다면 어떻게 되겠습니까?

한 부문에서 사용되고 있는 기술은 다른 부문에서 유래

기업은 정보를 전송하여야 할 의무를 지니기도 합니다(가령, 직원들에 대한 정보를 공공사회보장기관이나 국세청에). 공공기관은 민간 기업이 작성한 전화번호부나 기타 자원을 공개하여 사용하기도 합니다.

양 부문간에는 일상적으로 많은 정보 이동이 이루어집니다. 정보의 디지털화로 인해 심각해지는 민감한 문제들도 있습니다. 예를 들어, 민간단체가 다른 목적으로 공공기록의 사용을 꾀하기도 하고, 공공보안기관은 항공예약시스템, 통신기록, 인터넷 서비스 업체 기록에 대한 온라인 접속을 원하기도 합니다.

결론

정보공유로 인해, 정보 주체의 권리를 침해할 수 있는 허점을 막기 위해 DP 원칙의 적용에 있어 일관성을 유지하는 것이 매우 중요합니다. 일관된 원칙 적용이 없다면, 기본 개념은 공공 및 민간부문에서 상이하게 해석될 수 있습니다. 한 부문에서 특정한 보호를 받는 기록이 다른 부문으로 이동되어서는 그러한 보호를 받지 못할 수도 있습니다. 한 DPA가 조사중인 사안이 양 부문을 넘나드는 경우, 그 DPA가 양 부문에 대한 관할권이 없다면 제대로 기능을 수행할 수 없을 것입니다.

물론, DP 원칙의 적용에 있어 어느 정도 차이를 두는 것이 일부 경우에서는 적법할 수도 있지만, 적절한 해결책은 적절한 고려를 통해서만 가능할 것입니다.

II-2. 왜 DPA 감독기능과 기타 인권 감독기능을 통합하는 것이 가능하며, 그 기능들은 무엇인가? - 일관성과 효율성

DP권 외의 인권들도 독립적 기관에 의해 감독되어야 할 필요가 있습니다.

특히, 공공정보나 문서에 대한 민간부문의 접근권의 경우가 그렇습니다. DP권 감독과 접근권 감독을 병행하는 단일 독립기구를 설치한 국가들도 있습니다.

II-2.1. 공공정보나 문서에 대한 기본적 접근권 감독기능과 DP권 감독기능의 통합

두 권한 분야의 통합은, 공공정보에 대한 권리가 DP권에 앞서 확립된 캐나다 지방 정부(퀘벡을 비롯한 여러 주)에서 시작되었습니다. 오늘날에는 영국, 독일, 스위스와 같이 공공정보 접근권이 DP권 이후에 인정된 일부 유럽 국가에서도 이루어지고 있습니다. 프랑스의 경우, 정보 접근권은 DP권과 같은 해인 1978년에 확립되었지만, 여러 논의에도 불구하고 여전히 별도의 두 독립 기관이 존재합니다. 그러나, 최근에는 DPA 기관장이

독립적인 접근권 관할 기관(Access Authority)의 위원 1명을 지명할 수 있게 하는 등의 접근권 관련법 개혁을 통해 일관성을 확보하려는 움직임이 나타나고 있습니다.

국민의 공공정보 접근권은 특히 정보 요구자가 아닌 개인의 사생활을 보호하기 위한 면제항목(exemptions)을 포함하는 한편, 자신의 정보에 대한 개인의 접근권을 보장하고 있습니다. DP 원칙에서의 접근권은 접근성 원칙에서의 권리와 동일합니다.

공공정보는 그 내용이 무엇이던 간에 더욱 전산화되어가고 있으며, 새로운 공공 또는 민간 서비스를 위해 공공정보에 대한 온라인 접근 압력은 더욱 커지고 있습니다. 이러한 상황에서 DP권과 접근권 체제 사이의 더욱 긴밀한 조정이 요구되는 이슈들이 추가로 발생하고 있습니다. 접근권 관련법에 따른 제3자 정보 요청은 DP 규정에 의한 권리와 상충할 가능성도 있습니다.

II-2.2. 국민과 공공행정간 조정자로서의 옴부즈맨

상대적으로 규모가 작은 관할지역에서는 접근권과 DP권 감독기능을 옴부즈맨 기능과 절충하는 제도적 해결책을 발견할 수 있는데, 캐나다 뉴브런스윅 지방(인구 300,000명)이 그 예입니다. 이 방식은 향후에 자원이 제한되어 있는 개발도상국에서 효과적인 해결책이 될 수 있을 것으로 생각됩니다.

III- 왜 정보보호기관은 독립적이어야 하는가? 독립성은 어떻게 확보하는가?

III-1. 왜 독립성이 요구되는가? - DPA 기능의 특징과 더욱 더 근본적인 권리로 인정되고 있는 DP권의 특성

두 가지 주된 이유로 DPA는 정부로부터의 불편부당성과 독립성을 필요로 합니다.

첫 번째 이유는, 앞서 말한 바와 같이, 정부의 다른 두 독립기구인 의회와 사법부에 의존하지 않고 운영될 수 있는 더 신속하면서도 효율적인 방법이 필요하기 때문입니다. 실제로, DP 업무는 그 특성상 민주사회에서 공평하게, 그러므로, 독립적으로 수행되어야 합니다.

- DP 업무는, 관련된 경우, 특히 정책이나 인허가와 관련하여 특정 정보처리가 이루어지기 전에 의견을 제시함으로써 정부를 비판하는 일을 함축하고 있으며,
- 사후에는 심각한 권리의 침해가 있는 경우 조사를 실시하고, 중재하며 제재를 부과하거나 추진하는데, 이러한 기능의 수행을 위해서는 공평성, 독립성, 변호권 보장 절차 등이 요구됩니다.

두 번째 이유로, 유럽과 기타 대륙에서 DP권이 기타 인권에 대해 지니는 상관성과 함께, DP권의 인권적 성격이 최고 단계의 법규범에서도 점차로 인정되고 있습니다.

정보화 사회에서, DP권은 여타 기본권의 행사를 위한 안전장치를 제공합니다.

오늘날 회원에 관한 전자 파일을 작성하지 않는 노조, 인권단체, 정당 또는 교회가 있습니까? 이러한 단체 중에서 사회적 네트워크에 관한 그룹을 결성하지 않는 곳이 있습니까? 점점 더 많은 사람들이 블로그를 통해 자신의 생각을 공유하고자 하지 않습니까? 이동통신업체 중에서 통화 연결을 위해 자사 가입자의 위치 정보를 처리하지 않고 운영하는 곳이 있습니까? 어느 검색 엔진이 여러분의 관심사에 대해 알지 못하면서 여러분의 요구에 부응할 수 있겠습니까? 인터넷 서비스 제공업체가 여러분이 이용하는 웹사이트를 모르고 있을까요? 어느 의사, 병원 또는 사회보장서비스가 고객의 개인 정보를 처리하지 않고 일을 하고 있습니까? 미래에는 이러저러한 목적으로 모든 옷, 이동기기 또는 사람들에게 RFID칩이 붙여지지 않을까요?

이러한 모든 장치와 서비스는 우리의 기본권, 사생활, 결사, 종교적 신념, 자유로운 이동, 언론의 자유, 정보의 자유, 그리고 무엇보다도 존엄성과 자율성과 관련된 개인정보를 처리합니다.

따라서, 앞서 언급했던 다양한 남용 피해로부터 우리들을 보호하는 정보보호 및 사생활 보호 원칙과 방법은 실제로 사생활 외의 더 많은 것을 보호해 줍니다. 즉, 우리의 기본권 모두를 보호하고 있습니다.

이와 관련하여, 지금까지 구속력 있는 정보보호규정을 채택한 약 50개국의 최상 단계의 법규범에서 다음과 같은 동향을 살펴볼 수 있습니다.

EU의 경우, 27개 회원국 중에서 13개국이 헌법에서 정보보호를 기본권으로 명시하여 인정하고 있습니다. 특히, 포르투갈과 스페인에서 시작되어 동유럽 국가로 이어진 예에

서 처럼, DP 원칙이 인정된 후에 민주주의를 이룩한 국가들의 경우가 그러합니다. "오래된" 민주주의 국가에서는, 헌법재판소가 법리에 의해 DP권을 인정하여 왔으며, 특히, 독일은 1983년 이후로, 프랑스는 여러 경우를 통해 사생활 보호에 근거하거나 자유에 근거하여 그 권리를 인정하고 있습니다.

EU 차원에서 보면, 2001년 니스에서 개최된 국가수반 정상회의에서 선포된 'EU 기본권 헌장(EU Charter of Fundamental **R**ights)는 기본권으로서의 정보보호권을 명시적으로 인정한 최초의 지역/국제 문서입니다(제8.1조). 이 헌장은 몇 개월 이내에 리스본 조약(Lisbon Treaty)에 의해 완전한 효력을 갖게 될 것으로 보입니다. 더 나아가, 해당 조항은 이미 스트라스부르그에 위치한 유럽인권법원이 판결문에서 사용한 바 있습니다. 흥미롭게도, EU헌장에는 **독립적 기관에 관한 원칙이 포함되어 있어서, 그리스 헌법(9A조)이 이전에 최초로 그랬던 것과 같이 헌법 차원에서의 정책 가능성을 제기하고 있습니다.** 이 조항이 지니는 영향력을 보여주는 한 중요한 예로, 그 기원은 1999년에 이탈리아 DPA가 의장직을 맡아 EU DP 관계기관 그룹에서 채택한 구상안에서 비롯됩니다.

EU 회원국이 아닌 스위스의 경우에도 헌법에서 DP권을 인정하고 있습니다.

캐나다에서는, 최고 법원이 정보보호권을 기본권으로 인정하였습니다.

여타 국가들의 경우, 이와 동일한 경향이 나타납니다. 가령, 아프리카 베냉의 헌법개혁위원회는 2009년 초에 발표한 보고서에서 정보보호권을 헌법적 권리로 인정할 것을 권고하였습니다. 라틴 아메리카, 특히, 멕시코에서도 유사한 사업이 진행중입니다. 라틴 아메리카에서는, 1980년대 말과 1990년대에 여러 국가들에 영향을 미쳤던 민주화 이후로, 헌법 개혁을 통해 공공정보/문서 접근권의 도입이 이루어져 왔습니다. 개인정보에 대한 접근권도 'habeas data(인신보호 영장이라는 'habeas corpus'에 비견하여, 정보 주체가 자신에 관한 정보의 타당성을 심사하기 위해 열람할 수 있는 제도)'라는 흥미롭고도 혁신적인 개념에 의해 인정하여 왔습니다. 이를 기반으로, 일부 라틴아메리카 국가들은 DP 규정을 개발하였거나 현재 개발중에 있습니다.

EU 지침에 명시된 바에 의하면, DPA는 "부여된 기능을 수행하는 데 있어 완전히 독립적으로 활동"하여야 합니다(제28.1조). 독립성 요건은 이 지침을 이행하는 여러 국내법에 포함되어 있습니다. 이러한 국내법은 일반적으로 다음과 같은 특징을 지닙니다.

III-2.1. 기본적 공통 규정

DPA를 설치함에 있어, 회원국들은 대체로 1993년에 UN이 인권의 보호와 증진을 위한 국가기구의 지위와 관련하여 채택한 소위 “파리 원칙(Paris Principles)”에 포함되어 있는 원칙들을 따랐습니다.

- 직책 규정은 DP 관련법에서 명료하게 정하고 있으며, 직책은 공식 법규에 의해 효력을 지닌다.
- 임기 (회원국에 따라 4~6년으로, 모든 회원국에서 연임 가능)
- DPA가 합의체인 경우에는 협의 권한 이상을 지니게 되므로, 이익 상충을 해결하기 위한 규정이 마련되어 있다. (가령, 한 구성원이 자신의 이익에 관하여 위원장에게 선언하고 해당 구성원은 그러한 이익과 관련된 결정에 참여하지 못함)
- 위원이 위임을 받고 취한 행동에 대해서는 면책권이 제공된다.

III-2.2. 적격성과 독립성 보장을 위한 구성 및 지명 방식

DPA의 구성과 관련하여, EU에서는 두 가지 주요 모형으로 나누어지는데, 합의체 모형(collegial model)과 단독 감독관 모형(a single commissioner model)입니다. 구성원(들)의 지명도 정부와 사적 이권으로부터의 독립과 관련된 원칙을 따릅니다. 기본적으로, 일반적인 공공기관의 조직상 정체성(공화국, 입헌군주제, 봉건제 등)을 감안합니다.\

합의체 모형

합의체 모형은 보편화되어 있지만, 가장 일반적인 모형은 아닙니다. EU 회원국 중에서는 오스트리아, 벨기에, 불가리아, 프랑스, 이탈리아, 그리스, 룩셈부르크, 네덜란드, 포르투갈이 합의체 DPA를 두고 있습니다. EU 밖에서는, 부르키나파소, 퀘벡주, 멕시코, 모나코, 세네갈에서 이 모형을 채택하고 있습니다.

합의체 구성원의 규모와 자격은 다양한 배경과 집단을 대표하는 구성원들의 수, 인권과 기술적 사안을 처리하는 구성원의 능력에 따라 결정됩니다. EU에서는, 구성원의 수가 룩셈부르크와 네덜란드의 경우 3명에서부터, 이탈리아 4명, 포르투갈과 그리스는 10명 이상, 프랑스는 17명(17명 중에서 12명은, 의회 양원, 최고 행정부, 대법원, 회계법원

(Accounting Court), 사회경제위원회가 각각 2명씩 지명하고, 나머지 5명은 의회 양원의 의장이 각각 1명, 정부에서 3명을 지명함)에 이르기까지 다양합니다. 벨기에에서는 의회가 정부 추천 후보자 중에서 임명합니다. 이때 정부는 두 배수의 후보자를 추천하여야 합니다.

합의체 모형에서 독립성을 강화하기 위해, 프랑스의 경우와 같이 해당 기구의 위원장을 구성원 중에서 선출하거나 룩셈부르크와, EU 밖에서는, 모로코의 경우에서처럼 군주와 같은 상위 기구를 포함한 기타 수단을 통해 지명할 수 있습니다.

단독 감독관 모형

"단독 감독관" 모형은 그 밖의 EU 회원국에서 채택되고 있으며, 때로는 행정부가 단독 감독관을 임명하기 전에 독립적인 특별 배심원단을 구성하는 다양한 절차가 이용되기도 합니다. 이러한 지명은 의회가 직접 하는 경우가 점차 늘어나고 있습니다. 독일의 경우, 처음에는 정부가 연방 DPA를 지명하였지만, 현재는 의회에서 선출하고 있습니다. 독일 주에서도, 지방 의회에서 DPA 감독관을 선출합니다.

이 모형은 때로 1~2인의 부감독관을 지명함으로써 보완이 이루어지기도 하는데, 대체로 역량과 독립성을 보장하기 위한 절차가 포함됩니다. EU 체제에서는, 유럽집행위원회가 구성한 독립적인 특별 배심원단이 여론에 부응하는 후보자들을 대상으로 청문회를 실시한 뒤 명단을 작성하면 각료이사회와 유럽의회가 만장일치로 DP 의장(Supervisor)과 부의장(Deputy Supervisor)을 선정합니다.

특별 조항

사법 및 행정 체계에 따라, DP 관련법은 내외부로부터의 독립성 유지를 지원하기 위한 EU 특별 조항을 포함할 수 있습니다. 가령, 이러한 조항은 해당 DPA가 어떠한 명령의 대상도 되지 않으며 DP 구성원은 헌법재판소나 대법원에서 독립성 선서를 한다고 명시할 수 있습니다.

III-2.3. 자원의 충당과 규모

EU에서는 DPA의 예산이 투명하게 운영되며 정부로부터 독립성을 유지할 수 있도록 자체 인프라와 인력을 운용할 수 있습니다. 가령, 프랑스의 DPA는 예산이 연간 공공예산에서 구체적으로 다루어져 있어서 의회의 의결을 받아야 합니다.

지출 관련 결정은 어떠한 타 기관의 사전 승인도 거칠 필요가 없습니다(그렇지 않다면 DPA의 독립성이 침해될 수 있습니다). 지출 내역은 사후에 타 공공기관에 대해서와 마찬가지로 동일한 예산 감독 매커니즘을 통해 검토될 수 있습니다.

DPA 재정 규모는 회원국에 따라 상당한 차이를 보입니다. 특히, 프랑스 DPA 감독관은 더 많은 인력 확보를 위해 주기적으로 격론을 벌이는 실정입니다. 자금을 늘리기 위해, 기업의 통지 의무에 수수료를 부과하는 회원국들도 있습니다(영국, 벨기에).

III-2.4. DPA 업무에 대한 이해 증진

공공사업, 법안 또는 규정에 관한 DPA의 견해뿐만 아니라 연례보고서를 정기적으로 발간하는 일은 대중의 인식을 고취하기 위해 중요한 활동입니다. 이러한 활동은 DPA가 독립성을 확보하고 공정성을 증명하는 데에 도움이 됩니다. 제재 권한을 행사하는 경우에도 그러한 판정에 대해 널리 알리는 것이 필요합니다. 연례보고서 발간은 EU 지침에서 명시되어 있습니다.

결론

국가 및 EU 차원에서 효과적인 정보보호 감독 및 집행을 위해 필요한 기본적 기능들은 첫 번째 조정 단계(1995년 지침) 이전에 역사에 근거하여 신중하게 정해진 것으로 보입니다. 그렇다고 해서 모든 것이 완벽하다는 것은 아닙니다. 일부 회원국에서는 여전히 특정 부분에 결함이 존재하기도 합니다. 가령, 비밀 활동에 대한 권한이 제한되어 있다거나, 국가 하위 단계에서 여러 부문에 대해 여러 기관이 존재한다든가, 정부 사업에 대

한 DPA의 사전 의견을 제기할 수 없거나 그러한 의견에 대한 홍보가 부족하다든가, 현장 단속을 위해 사전에 기업의 동의를 얻어야 하는 등의 문제가 있습니다. 그러나, 모든 회원국의 경험을 통해 DPA 기능과 활동에 대해 지속적인 정보가 제공되는 학습 과정이 이루어지고 있습니다.

EU 회원국의 DPA 구조는 회원국의 정부 조직에 관한 상이한 전통에 따라 매우 큰 차이를 보이기는 하지만, 이러한 다양한 구조를 통해 국가 및 EU 차원에서 효과적인 DP권을 지속적으로 증진할 수 있는 전략과 방법을 개발해낼 수 있습니다. 이러한 전략도 또한 학습 과정을 거치면서 발전하게 됩니다.

물론, 효율성은 가용자원에 따라 결정되며, 일부 경우에는 이러한 자원이 상당히 부족하기도 합니다. 자원 제약은 DPA가 자체 권한을 행사하는 데 있어 교육기관 및 연구기관과 제휴를 결성하고 모든 이해당사자, 정부, 의회, 업계 및 NGO로부터 최대한의 정보를 제공 받고 그들과 교류할 수 있는 역량을 저해합니다.

개인의 권리 보호 수준과 관련하여 DPA의 효율성 및 실효성을 평가하는 것은 이 글의 주제에서 벗어나는 일입니다. 그러나, 전반적으로 볼 때, 911 테러 직후와 같이 안보 문제에 대한 우려가 심각한 기간에는 DPA가 자유를 제한해서는 안 된다는 논의에 기여하거나 심지어 그러한 논의를 주도해나가기에 가장 적법한 기관으로 간주될 수 있습니다. 그러한 안보 상황에서는, 대부분의 경우 보안 파일의 범위를 확대하거나, 민감한 정보를 더 많이 수집하거나, 개인을 새로운 범주로 분류하거나, 정보 보유기간을 늘리거나, 비디오 감시와 같은 더 침해적인 기술을 도입하기 위한 부적절한 방안들이 제시됩니다. 그러한 상황에서, 독립적인 DPA의 공개적 견해는 더욱 큰 중요성을 지니게 됩니다.

제3국으로의 정보 이동과 관련법에 관한 규정은 EU 내에서 처리되는 정보의 주체인 EU 회원국 국민, 거주민, 재외 국민 모두의 DP권을 보장하고 있습니다. 그러나, 인권이라는 일반적인 관점에서 볼 때, 그리고 특히 효율성을 위해서는, DP 규제는 현재 일관성에 있어 미흡한 만큼 전지구적 차원에서 상당한 개선을 필요로 합니다. 아직까지 정보보호 규정을 채택하지 않은 국가는 100개국이 넘으며, 현재의 국제 기제에는 적절한 독립적 모니터링이나 조율된 집행 기능이 명시되어 있지 않습니다. 모든 이해당사자들의 시급한 노력이 없다면, 이러한 문제들을 개선하기 위해 모든 DPA가 현재 펼치고 있는 다각적 노력이 조속한 시일 내에 성공을 거두기는 힘들 것입니다.

한국에서의 개인정보보호관련 쟁점 및 개인정보보호기구의 역할과 위상

염흥열 (순천향대 정보보호학과 교수)

1
토 론

Personal information protection issues and the role and position of data protection authorities in Korea

Youm, Heung-Youl
(Professor at the Department of Information Security in Soonchunhyang University)

At this highly information-based society where there is **a growing need of personal information handling**, including collection, use and disclosure of personal data, to provide individuals with a range of administrative and information services, there also exists **a greater risk of abuse/misuse or illegal use of personal information** due to the nature of easy and speedy distribution of such information driven by the digital techniques, which **increases the significance of personal information protections** to secure privacy of the data subjects. This is why, in Europe and some countries of the Asia-Pacific region, efforts have been made to create or improve the legislation for personal information or privacy protection in order to ensure an adequate coordination of the rights of personal information processing and request and the conflicting rights.

I would like to start by informing you that this paper is totally based on my technical background, experiences and common sense as an engineer. I also want to say that it is a great honor for me to have a chance to exchange views on the role and position of an institution protecting individual privacy, especially with Graham Greenleaf, Professor at University of New South Wales in Australia and Marie Geroges, Informatics and Liberties Consultant, whose authority in the area of privacy protection is internationally respected.

I am very impressed with the keynote speech by Marie GEORGES, which is enriched with her extensive experiences and expertise in the field of personal information protection or data protection. In the speech, she sets out the essential functions of a supervisory body for personal information protection; the significance of establishing a supervisory body covering

both the public and private sector; the need to establish an independent supervisory body free from the pressures from government ministries and other stakeholders; a range of requirements to ensure independence of such body, including a fixed term; and the types of such supervisory body. I would say that I agree with her in many respects.[1)]

I also find the presentation by Professor Graham Greenleaf very impressive. **The factors relevant to an overall assessment of independence** of the data protection authorities (DPAs), **the international standards** for DPAs' independence and **the experiences in the Asia-Pacific region** concerning the powers and structure of a DPA are very informational. In addition, **the lessons learnt from those experiences** are reasonable and I share the same view. In particular, I agree with his findings for the **need to establish a supervisory body satisfying the independence requirements, extend its scope of activities to cover both the public and private sector and establish a multi-member commission for data protection.**[2)]

Still, it is important to note that an enactment is **the outcome of compromise and agreement among the different classes of stakeholders** in the economy and society, and considerations should be made about the past and present **social and cultural circumstances and the legal practices and traditions** of a particular society.

This paper includes the following: **Chapter 1** gives **a general picture on the enaction of data protection provisions included in individual laws or a comprehensive specific law** and **analyzes the three bills on personal information protection which are under review in the Parliament**; **Chapter 2 analyzes the three bills using the general and specific criteria** to assess the DPAs' independence; and **Chapter 3** proposes **considerations an orientations for domestic legislation**; and **Chapter 4** gives **a conclusion**.

---

1) Marie GEORGES, "History, Structure, and Functions of European Independent Data Protection Supervisory Authorities," National Human Right Commission of Korea, Symposium on Analyzing the role and position of an Institution Protecting Individual Privacy, September, 2009.

2) Graham Greenleaf, "Independence and power of data protection authorities: International Standards and Asia-Pacific Example," National Human Right Commission of Korea, Symposium on Analyzing the role and position of an Institution Protecting Individual Privacy, September, 2009

Chapter 1. Analyzing the developments in personal data protection legislation in Korea

1.1 Developments in personal data protection legislation

At present, the personal data protection provisions for the public and private sector (information and telecommunications, finance, health, etc.) are contained in different individual laws which are administered by relevant government ministries. The individual laws applicable to different areas are summarized in Table 1 below[3]:

Table 1 Individual laws for personal information protection in different areas

Area	Major legislation	Responsible Ministry
Public administration	Public Agency Data Protection Act	Ministry of Public Administration and Security
Information & telecommuni-cations	Act on Promotion of Information and Communications Network Utilization and Information Protection	Korea Communications Commission
Medical service	Basic Act on Health and Medical Care; Medical Care Act	Ministry for Health, Welfare and Family Affairs
Credit/finance	Act on Use and Protection of Credit Information	Ministry of Strategy and Finance
Education	Basic Education Act	Ministry of Education, Science and Technology

Given that personal information is protected and handled under a range of individual laws in Korea, there might be **blind spots of law application** that are beyond the coverage of those

3) Parliamentary Committee on Administrative Security, the Documents for Public Hearing on the Bills on Personal Information Protection, April 2009.

laws, and there exist **different levels of data processing and of penalties for breaches** of the laws. This is why there have been persistent proposals for a comprehensive act on personal information protection to regulate the overall data processing in this country which may resolve the aforementioned problems. Since 2005, efforts have been made **to enact a comprehensive law protecting personal information** in order to define a coordinated regulation of data processing and remove the legal loopholes. As a consequence, three bills on personal information protection were brought before the Parliament for deliberation. However, **none of them have been adopted for legislation yet, largely because lawmakers have failed to reach agreement on the role and positions of a supervisory body for data protection.**

1.2 Analyzing the bills under Parliamentary review

Currently, three bills on personal information protection have been submitted to the Parliament: **the Draft act proposed by Ms. Hye-hoon Lee** from the ruling National Grand Party; **the Draft act proposed by Mr. Jae-il Byun** from the largest opposition Democratic Party; and **the Draft act proposed by the Ministry of Public Administration and Security (MoPAS)**.

These bills are pending in the Parliament, and it is totally left to the lawmakers which of the three will be the winner and what the chosen bill will be like in the final version.

The future law protecting personal information would be, in its nature, **a combination** of the European and the US laws. **The personal information protection legislation in Europe is based on a single comprehensive law covering all areas of business activities, whereas the US provides different general regulations for different sectors, with individual Ministries being responsible for data protection in the relevant areas**.

In general, the three bills share the similar legislation principles as described below, although they greatly differ from each other in the aspect on how to secure independence in terms of enforcement regime:

- The law should provide a higher level of personal information protection in each of the stages of data collection, use and disclosure than the existing individual laws, by **incorporating, as fully as possible, the OECD-defined eight principles** for personal information protection, including collection limitation principle and purpose specification principle, and **the international standards required by the international community** including EU and OECD, while **taking into account the particular circumstances of Korea such as social and cultural tradition and statutes and regulations.**

- The law should **coordinate the levels of protection, use and processing of personal information and the levels of penalties for breaches,** in order to ensure coherence and equitability among different individual laws, including 'Public Agency Data Protection Act' and 'Act on Promotion of Information and Communications Network Utilization and Information Protection'.

- The law should provide **clearer principles of personal information processing and stronger rights of individuals (data subjects)** at each and every stage of personal information processing.

- The law should **have an extended coverage** to include the Parliament, Courts, constitutional agencies and non-profit organizations such as communities and Internet-based cafes, to which the existing laws do not apply, and introduce **the standards for installation of CCTVs and protection from their abuse**, including the requirement of notices and the ban on recording.

The key contents of the bills under the Parliamentary deliberation are summarized in Table 2 below:

Table 2. Key contents of the three bills

	Hye-hoon Lee draft	Jae-il Byun draft	Government draft
General enforce-ment system	- Independent supervisory body - Personal information dispute mediation committee	- Independent supervisory body - Personal information dispute mediation committee	- Secretariat as part of a government ministry + personal information protection Committee - Personal information dispute mediation committee
Coverage	- Private + public	- Private + public	- Private + public
Key provisions	- Reinforcement of self regulation - Guarantee of the rights of data subjects - Personal information impact assessment - Personal information handling based on the consents of data subjects - Stricter limits on handling sensitive data - Standards for installation and operation of CCTVs - Special clauses on public agencies - Personal information dispute mediation	- Stronger principles for personal information processing - Transparency and impartiality in data processing - Guarantee of the rights of data subjects - Limits on automated processing, including by CCTVs - Personal information impact assessment - Promotion of self-regulation - Special rules for public sector - Group proceedings over personal information - Personal information dispute mediation	- Protection standards for each of the stages of data collection, use and disclosure - Stricter limits on processing of PII (personally identifiable information) - Limits on installation of CCTVs - Personal information impact assessment - Personal information dispute mediation - Registration and publication of personal information files in public agencies - Notification of personal information outflow - Stronger rights of data subjects - Appealing complaint on privacy violations

Chapter 2. Analyzing the bills in the context of independence of the personal information protection authorities

The general evaluation criteria which may be used to assess the three bills in the context of the independence nature of the authorities are summarized as below[4]:

- **Enforcement structure**
  . Independent supervisory body for privacy protection
  . Part of a government department
- **Functional independence**
  . Independent function with data protection alone
  . Combined function with other functions
- **Organizational structure**
  . Sole commissioner
  . Multi-member commission

Table 3 below shows an assessment of the three bills based on the evaluation criteria given above:

Table 3. Comparative analysis on three bilss, based on the general evaluation criteria

	Lee draft	Byun draft	Government draft
Enforcement structure	- **Independent commission** . Independent supervisory body under Prime Minister and a secretariat . Personal information protection committee	- **Independent commission** . Independent supervisory body under President and a secretariat . Personal information protection committee	- **Part of a government ministry** . Secretariat under MoPAS . Personal information protection committee under Prime Minister
Functional independence	- **Independent function** . Personal information protection function alone	- **Independent function** . Personal information protection function alone	- **Combined functions** . Activities of a responsible agency + personal information protection work
Composition	- **Multi-member commission**	- **Multi-member commission**	- **Multi-member committee**

4) Graham Greenleaf, "Independence and power of data protection authorities: International Standards and Asia-Pacific Example," Symposium on Analyzing the role and position of an Institution Protecting Individual Privacy, National Human Right Commission of Korea, September, 2009

	Lee draft	Byun draft	Government draft
Role of the commission/ committee	- **Policy establishment and enforcement**	- **Policy establishment and enforcement**	- MoPAS . Policy establishment and enforcement - **Personal information protection committee** . Consultation and advice
Coverage	- Public + private sector	- Public + private sector	- Public + private sector
Detailed functions of the commission/ committee	- **Policy establishment and enforcement** - Examining laws, institutions and practices - studies and updating - **Formulating and publishing criteria** - **Ombudsmanship, remedies and dispute settlement** - Fact-finding research and studies - Supporting and distributing technological innovations - Education and publicity - Promoting self-regulation - Exchanges and cooperation with international or foreign bodies	- **Establishing and enforcing mid- and long-term plans and annual plans** - Research and studies on facts and practices, and updating - Research and studies on laws and institutions, and updating - **Formulating and publishing criteria** - **Power to investigate and handling of complaints** - **Dispute settlement and remedies** - Supporting and distributing technological innovations - Education and publicity - Exchanges and cooperation with international or foreign bodies	- **MoPAS** . **Policy establishment and enforcement** - **Personal information protection committee** . **Framework plan and enforcement plan** . **Improving policies, institutions and legislation** . **Coordinating the different opinions of public agencies** . Interpretation and application of the legislation . Matters concerning use and disclosure of personal information . Matters concerning **personal information impact assessment** . Matters concerning **enforcement notices** . Publishing the handling outcomes

How independent a supervisory body for personal information protection is could be measured with these 13 evaluation criteria[5]:

5) Graham Greenleaf, Independence and power of data protection authorities: International Standards and

- **Establishment by law;**
- **Independent investigation power;**
- **Fixed term of office;**
- **Removal from office only for defined reasons;**
- **Immunity against personal law suite relating performance of official duties;**
- **Appointment by Parliament rather than by the Executive;**
- **Resources of the authority determined independently of the Executive;**
- **Powers and dutiesto report regularly to the Parliament;**
- **Co-appointment to a position which continues for some time after the term within the authorities expires (e.g. a Court committee);**
- **Preventing commissioners from undertaking other positions and requiring in multi-member commissions the disclosure of interests;**
- **A sole commissioner or multi-member commission;**
- **Combination with other authorities such as an Ombudsman or the National Human Rights Commission; and**
- **Part of a broader human rights authority**

Table 4. Comparison and assessment of the three bills based on the evaluation criteria

	Lee draft	Byun draft	Government draft
Legal foundation for the authority	- **Satisfied**	- **Satisfied**	- **Satisfied**
Fixed term for Commissioner/members	- **Satisfied** . 3 years and renewable once	- **Satisfied** . 3 years and renewable once	- **Satisfied (Chairman and members)** . 2 years and renewable once

Asia-Paciffic Example, Symposium on Analyzing the role and position of an Institution Protecting Individual Privacy, National Human Right Commission of Korea, September, 2009

	Lee draft	Byun draft	Government draft
Removal from office only for defined reasons	- **Satisfied**	- **Satisfied**	- **Partially satisfied** . To be prescribed in the Presidential Decree (presumably)
Immunity against personal law suit relating performance of official duties	- Not satisfied	- Not satisfied	- Not satisfied
Appointment by Parliament	- **Not satisfied** (Appointed by President) . Composed of 1 Chairman and 9 members including 1 standing member . The Chairman is to be appointed by President at the nomination by Prime Minister.	- Partially satisfied (Appointed by the heads of Legislature, Judiciary and Executive) . 3 members by Parliament; 3 by Supreme Court and 3 by President . Chairman is to be appointed by President.	- Not satisfied (Appointed by Prime Minister) . Composed of Chairman and 15 members or so. . Chairman is appointed by Prime Minister.
Duties to report annually to the Parliament	- **Satisfied**	- **Satisfied**	- Not satisfied
Co-appointment to a position which continues for some time after the term expires	- Not satisfied	- Not satisfied	- Not satisfied
Prevention of Commissioners undertaking other positions	- Satisfied (presumably)	- Satisfied (presumably)	- None applicable . Non-standing members
Composition	- **Multi-member commission**	- **Multi-member commission**	- **Multi-member committee (Coordination and dispute settlement)**
Combination with other authorities?	- **Independent function**	- **Independent function**	- None applicable

	Lee draft	Byun draft	Government draft
Part of a broader authority?	**- Separate organization**	**- Separate organization**	**- Part of a government ministry**

Table 4 above shows an analysis on the three bills, based on the specific criteria of assessment in terms of independence.

To sum up, as indicated in the analyses of Tables 3 and 4, the independence of the supervisory authority which is measured with the general and the specific criteria for evaluation is **the strongest in the Jae-il Byun draft and almost equally strong or slightly less in the Hye-hoon Lee draft and the weakest in the government draft.**

Chapter 3. Considerations/orientations for domestic legislation of personal information protection

Unarguably, the independence of a supervisory authority for personal information protection is one of the most important factors for enactment of the privacy protection law, but it is not all. I do think that it is possible to create a supervisory body with strong independence so as to perfectly secure privacy protection for data subjects. However, it is necessary to make additional considerations about the social, cultural and environmental factors described below, in facilitating the legislation for public information protection:

- It should be noted that the ongoing legislative efforts involve a process from the existing system with different laws applicable different areas towards an improved version of comprehensive legislation. Accordingly, the draft bills pending the Parliament should be considered **as being of an incremental design, not of a clean slate design.**

- A proper regard should be given to the economic and social circumstances and **the legislative practices and traditions in Korea**, and it should be ensured that the personal information protections are commensurate with the international standards and the advanced institutions in other countries, with **the best practices in Europe and the Asia-Pacific region** being in full consideration.
  . At present, **the Ministry of Public Administration and Security (MoPAS) governs the personal information protection in the public sector; the Korea Communications Commission, in the area of information and telecommunications;** and other Ministries, in their relevant area.

- President Lee, Myung-bak's Government is aiming for **a smaller but more efficient government** and is focusing on **deregulation** based on business-friendly policies.

- I find somewhat reasonable the argument that a multi-member committee should be formed within the Government as a supervisory body which **removes the potential conflicts among the government ministries.** It is also feasible, in terms of cost effectiveness, **to integrate the privacy protection function into a broader authority with similar functions,** such as the National Human Rights Commission, although this possibility is not considered in any of the three bills.

- The argument also needs to be considered that, given that the MoPAS has a great potential, due to the nature of its activities, to violate privacy and accordingly should be subject to the supervision for privacy protection, **it is inappropriate, in terms of objectivity, impartiality and transparency,** for the Ministry to serve also as a supervisory body. I think, however, that this inappropriateness could be resolved, although not completely, by way of **the Parliamentary supervision and check** through the annual reporting obligation, the **audits** by the Board of Audit and Inspection or self-regulation by the Ministry.

- It is also worthwhile to consider **the argument that establishing a supervisory authority for personal information protection independent of the government ministries is a necessary and sufficient condition to accomplish personal information protection. Even when the supervisory authority is established as part of a government ministry, it is necessary to set up long-term plans to strengthen its functional independence by increasing the powers of the authority and the independence of the membership**. In this light, one of the possibilities is to set up a personal information protection committee specifically in charge of privacy protection within the MoPAS.

Chapter 4. Conclusion

I believe that the need to enact a comprehensive law on personal information protection, instead of the existing dispersed system of individual laws, has **obtained the public consensus** and is **a pending issue** of great urgency. Now is the right time for **lawmakers to reach agreement at the earliest time possible,** based on the efforts and accomplishments they have made so far to legislate a privacy protection law. I hope that the presentations and discussions in this symposium will **give momentum to the ongoing process for legislation and provide a crucial turning point to speed up the process**. I would like to close my presentation by expressing my wish that the personal information protection legislation will be completed by the end of this year. I also would like to give special thanks to Ms. Marie Georges and Professor Graham Greenleaf for the eminent insights in their presentations.

1
토 론

한국에서의 개인정보보호관련 쟁점 및 개인정보보호기구의 역할과 위상

염흥열 (순천향대 정보보호학과 교수)

고도 정보화 사회에 진입함에 따라 정보주체에게 다양한 행정 및 정보 서비스를 제공하기 위해 개인정보 수집(collection), 이용(use), 삼자제공(disclosure) 등의 **개인정보 처리(handling) 필요성이 증대**되면서, 더불어 디지털 기술의 활용을 통한 개인정보의 쉽고 빠른 전파 특성에 기인한 **개인정보의 오남용(abuse/misuse), 악용(illegal use) 가능성이 점차로 증대**되고 있다는 점에서, 정보주체(Individual)의 프라이버시 보호하기 위한 **개인정보보호의 중요성이 더욱 강조**되고 있다. 유럽과 아시아·태평양 지역의 주요 나라에서도 개인정보 처리권과 요구권의 서로 충돌하는 권한에 대한 적절한 수준의 타협점을 제시하기 위해 개인정보보호 또는 데이터보호를 위한 법제도를 마련해 왔고 개선하고 있는 중이다.

저는 공학자로써 저의 기술적 배경과 경험 그리고 상식에 기반해 이 자료를 준비했음을 미리 알려드린다. 또한, 개인적으로 개인정보보호 분야에서 세계적으로 권위를 인정받고 있는 호주 New South Wales의 Graham Greenleaf 교수님과 Informatics and Liberties의 Marie GEORGES 자문관님과 함께 **개인정보보호 감독기구에 대한 위상과 역할**에 대해 토의할 수 있는 기회를 가질 수 있어 무한한 영광으로 생각합니다.

먼저 Marie GEORGES 자문관님의 지난 수 십년 간의 프랑스와 유럽에서 **개인정보보호(personal information protection) 또는 데이터 보호(data protection)** 분야에서 경험과 해박한 지식에 바탕으로 **개인정보보호감독기구의 필수 기능 제시**, **공공과 민간을 포함한 개인정보보호감독기구 수립**, 정부부처 및 관련 이해당사자로부터의 **독립성이 요구되는 감독기구 수립**, 감독기구의 독립성을 보장하기 위한 임기 보장 등의 **다양한 요구사항 및**

감독기구의 형태 등을 다룬 기조발표는 매우 인상적이었고, 많은 주장이 저의 견해와 일치함을 인정합니다.[1)]

또한, Graham Greenleaf 교수님이 발표하신 데이터 보호 감독기구(data protection authorities) **독립성 평가기준**, 감독기구의 독립성을 위한 **국제사회의 표준**, 감독기구의 구조와 권한 등에 대한 **아시아•태평양 지역의 겸험** 등은 매우 인상적이었으며, 또한 **이러한 경험을 통해 얻어진 교훈(lesson)은** 타당하고 저의 견해를 같이 하고 있습니다. 특히, **독립성 요구조건을 만족하는 감독기구 수립, 공공과 민간 부문을 포함한 감독기구 업무 영역, 복수 위원으로 구성되는 감독기구의 구성 필요성** 등에 대한 주장은 매우 타당하다고 생각합니다.[2)]

그럼에도 불구하고, 법제정(enactment)은 당시 경제•사회를 구성하는 **다양한 이해당사자(stakeholder)들의 타협(compromise)과 합의(agreement)의 결과**이며, 각 나라의 과거 및 현재의 **사회문화적 환경과 법제도의 관행•전통**을 고려해야 할 것 입니다.

본 발표는 다음과 같이 구성되어 있습니다. **제1장**에서는 **개별법에 근거한 개인정보보호법 및 포괄적인 개인정보보호법 입법화 현황**을 제시하고 **국회에서 심의중인 3가지 개인정보보호법 후보 법안을 분석**하고, 제2장에서는 개인정보보호감독기구의 독립성을 평가하기 위한 **일반 및 세부 평가기준을 이용해 3가지 개인정보보호 후보 법안에 대해 분석**하며, 제3장에서는 **국내 입법화를 위한 고려사항/추진방향을 제시**하고, 제4장에서 결론을 맨도록 하겠습니다.

---

1) Marie GEORGES, “History, Structure, and Functions of European Independent Data Protection Supervisory Authorities,” National Human Right Commission of Korea, Symposium on Analyzing the role and position of an Institution Protecting Individual Privacy, September, 2009.

2) Graham Greenleaf, “Independence and power of data protection authorities: International Standards and Asia-Pacific Example,” National Human Right Commission of Korea, Symposium on Analyzing the role and position of an Institution Protecting Individual Privacy, September, 2009

제1장 국내 개인정보보호법 입법화 현황 분석

1.1 국내 개인정보보호 법제 현황

현재 국내 개인정보보호 법제는 공공·민간(정보통신, 금융, 보건 등) 분야별로 여러 다른 개별법에 근거하여 각 소관 부처별로 개인정보처리행위를 규제하고 있다. 이를 요약하면 [표 1]과 같다.[3)]

[표 1] 개인정보보호를 위한 분야별 개별법

분야	주요 법안	소관 부처
공공행정	공공기관의 개인정보보호에 관한 법률	행정안전부
정보통신	정보통신망 이용촉진 및 정보보호 등에 관한 법률	방송통신위원회
의료	보건의료 기본법, 의료법	보건복지가족부
신용/금융	신용정보의 이용 및 보호에 관한 법률	기획재정부
교육	교육기본법	교육과학기술부

다양한 개별법에 근거하여 보호 및 처리(handling)되고 있는 국내 개인정보보호 환경은 개별법이 미치지 못하는 **법 적용의 사각지대**(blind spot)**가 존재**할 수 있고, 개인정보보호 처리 수준 그리고 위반으로 인한 **처벌(penalty) 수준이 상이하는 등 문제점**이 노출되고 있다. 따라서 이러한 문제점(problem)을 극복하기 위하여 국가사회 전반의 개인정보 처리를 규율하기 위한 포괄적 개인정보보호법 제정 필요성이 줄기차게 요구되어 왔습니다. **포괄적 개인정보보호 법 제정(enactment)**은 균형적인 개인정보 처리 수준을 규정하고 법적용의 사각지대를 없애기 위하여 2005년부터 추진해 왔고 현재 국회에 3가지 후보 법안이 상정되어 심의(deliberation) 중에 있는 실정입니다. 그러나, 주로 **감독기구의 위상(position)과 역할(role) 등의 항목에서 합의에 이르지 못해 2009년 9월 현재 법제화가 완성되지 않고** 있는 실정이다.

3) 국회행정안전위원회, 개인정보보호법안에 대한 공청회 자료집, 2009.4

1.2 국회에서 입법화를 추진 중인 개인정보보호 후보법안 분석

현재 국회에서 개인정보보호법 제정을 위해 3가지 후보 법안이 상정되고 심의중이며, 이는 집권 여당인 한나라당(National Grand Party) 의원 중심으로 제안된 **이혜훈의원안** (Draft act proposed by Ms. Hye-hoon Lee), 제1야당인 민주당(Democratic Party) 의원을 중심으로 제안된 **변재일의원안**(Draft act proposed by Mr. Jae-il Byun), 그리고 행정안전부(MoPAS, Ministry of Public Administration and Security)가 제안한 **정부안**(Draft act proposed by MoPAS) 등이다.

현재 이 세 가지 안이 국회에 계류(pending) 중이며, 아직 3가지 후보 법안중 어떤 법안이 최종적으로 선택될지, 선택된 법안의 최종 형태는 어떤 모양일지는 입법자(law makers)의 판단에 남겨져 있다고 볼 수 있습니다.

먼저 현재 추진되고 있는 국내 개인정보보호법의 성격을 살펴보면, **유럽**의 개인정보보호법 체제가 **포괄적이면서 하나의 법에 기반하여 모든 비즈니스 영역을 규제**하고 있고, **미국**의 개인정보보호 법체제가 부문별 **일반 규제이며 개별 부처 차원에서 데이터 보호를 법제화 및 시행**하고 있는 반면, **한국**이 현재 추구하고 있는 개인정보보보호법은 포괄적인 **유럽의 법체계와 부문 기반의 미국의 법체계를 결합한 절충 형태(combined form)의 법체계**를 추구하고 있다고 볼 수 있다.

대체적으로 세가지 안이 대체적으로 다음과 같은 유사한 **입법 원칙**을 갖고 구성되어 있으나, 추진체계의 독립성 확보 측면에서 가장 큰 차별을 보이고 있다.

- 수집제한원칙(collection limitation principle), 이용목적명세(purpose specification principle) 등을 포함하는 OECD에서 정의한 개인정보보호 8대 원칙과 EU와 OECD 등의 **국제 사회가 요구하는 국제적인 표준 원칙들을 최대한 반영**하면서, **국내 사회·문화적 전통과 법령·제도(statutes and regulations) 등의 환경을 고려**하여 수집, 이용, 삼자제공 등의 각 단계에서 기존 개별법보다는 강화된 개인정보보호 수준을 제공한다.

- '공공기관의 개인정보보호에 관한 법률' 과 '정보통신망 이용촉진 및 정보보보 등에 관한 법률“ 등의 개별 법제 상호간에 일관성과 균형성을 유지하기 위해 **개인정보 보호와 처리, 이용 등의 수준과 처벌 수준의 균형**을 유지한다.

- 각 개인정보 처리 단계마다 **개인정보 처리원칙의 명확화와 이용 주체의 권리를 강화**한다.

- 개별법에서 적용되지 못해 왔던 국회, 법원, 헌법 기관 등과 동호회 및 인터넷 카페 등의 비영리 단체로의 **법 적용 범위를 확대**하고, 안내판 설치와 녹음 금지 등 **영상정보처리(CCTV) 설치 및 이용 보호 기준**을 새로 도입한다.

현재 국회에서 심의중인 세 후보 법안의 주요 내용은 [표 2]와 같이 요약될 수 있다.

[표 2] 3개 후보 법안의 주요 내용

	이해훈의원안	변재일의원안	정부안
추진체계 일반	- **독립 감독기구** - **개인정보분쟁 조정위원회**	- **독립 감독기구** - **개인정보분쟁조정위원회**	- **행정부 소속형 사무국 + 개인정보보호위원회** - **개인정보분쟁조정위원회**
적용범위	- 민간 + 공공	- 민간 + 공공	- 민간 + 공공
주요 내용	- 자율규제(self regulation)의 강화 - 정보주체의 권한 보장 - **개인정보영향평가 (impact assessment)** - 정보주체 동의 기반 개인정보 처리(handling) - **민감정보(sensitive data) 처리 제한 강화** - **영상정보처리기기 설치운영 기준** - **공공기관 특례규정** - **개인정보분쟁조정 (dispute mediation)**	- 개인정보 처리 원칙 강화 - 투명하고 공정한 개인정보 처리 - 정보주체 권리 보장 - **영상정보처리기기를 포함한 자동화기기의 처리 제한** - **개인정보영향평가 (impact assessment)** - 자율규제의 촉진 - 공공부문 특칙 - 개인정보 단체소송 - **개인정보분쟁조정 (dispute mediation)**	- 개인정보의 수집, 이용, 제공 등 간계별 보호기준 마련 - **고유식별정보(PII, personally identifiable information)의 처리제한 강화** - **영상정보처리기기 설치 제한** - **개인정보보호 영향평가** - **개인정보분쟁조정 (dispute mediation)** - **공공기관 개인정보 파일의 등록 및 공개** - 개인정보 유출 사실 통지 - 정보주체의 권한 강화 - **개인정보 침해사실 신고 (appealing complaint)**

제2장 개인정보보호감독기구의 독립성 측면에서 후보 법안 분석

독립성 측면에서 세 가지 후보 법안을 평가하기 위한 **일반 평가 기준(evaluation criteria)**은 다음과 같이 요약될 수 있다.[4)]

- **추진체계(enforcement structure)**
  . 독립 프라이버시보호감독기구
  . 정부 부처 소속형(part of government department)
- **기능(function) 독립성**
  . 독립형(independent function with data protection alone)
  . 결합형(combined function with other functions)
- **위원구성 형태**
  . 독립 감독관형(sole commissioner)
  . 다수 위원형(muit-member commission)

위에서 제시된 일반 평가 기준을 근거하여 세 후보 법안을 평가하면 [표 3]과 같다.

[표 3] 일반 평가기준에 의한 세 후보 법안 비교분석

	이해훈의원안	변재일의원안	정부안
추진체계(enforcement structure)	**- 독립 감독기구 (independent commission)** . 국무총리 소속 독립 감독기구, 사무처 수립 . 개인정보위원회	**- 독립감독기구 (independent commission)** . 대통령소속 독립 감독기구, 사무처 수립 . 개인정보보호위원회	**- 정부부처 소속형(part of government agency)** . 행정안전부 소속 사무국 . 국무총리 소속 개인정보보호위원회
기능 독립성	**- 독립형 (independent function)** . 개인정보보호 기능만	**- 독립형 (independent function)** . 개인정보보호 기능만	**- 결합형 (combined functions)** . 소관부처 고유 업무 + 개인정보보호 업무

4) Graham Greenleaf, "Independence and power of data protection authorities: International Standards and Asia-Pacific Example," Symposium on Analyzing the role and position of an Institution Protecting Individual Privacy, National Human Right Commission of Korea, September, 2009

	이해훈의원안	변재일의원안	정부안
위원 구성	- **다수 위원으로 구성된 감독기구 (multi-member commission)**	- **다수 위원으로 구성된 감독기구 (multi-member commission)**	- **다수 위원으로 구성된 심의 위원회 (multi member committee)**
감독기구/ 위원회 역할	- 정책 수립 및 집행 기능 (policy establishment and enforcement)	- 정책 수립 및 집행기능 (policy establishment and enforcement)	- 행정안전부 . 정책수립 및 집행 (policy establishment and enforcement) - **개인정보보호위원회** . 정책 심의 및 자문 (consultation and advice)
적용 범위	- 공공(public sector) + 민간 부분(private sector)	- 공공 + 민간 부분	- 공공 + 민간 부분
감독기구/ 위원회 세부 기능	- **정책의 수립 및 시행** - 법, 제도, 관행 조사 - 연구 및 개선 - **기준의 제정 및 고시** - **고충 처리(Ombdsmen) 및 피해 구제(remedies) 및 분쟁조정(dispute settlement)** - 실태 조사 및 연구 - 기술개발의 지원 및 보급 - 교육 및 홍보 - 자율규제활동의 촉진 - 국제 기구및 외국 기구와의 교류 및 협력	- **중장기 계획 및 연차계획 수립 및 시행** - 실태 및 관행 조사, 연구 및 개선 - 법령, 제도 등의 조사, 연구 및 개선 - **기준의 제정 및 고시** - **사건의 조사(power ot investigate) 및 고충 및 진정의 처리(handling of complaints)** - **분쟁 조정 및 구제** - 기술개발의 지원 및 보급 - 교육 및 홍보 - 국제기구와 외국 기구와의 교류 및 협력	- **행정안전부** **. 정책 수립 및 시행** - **개인정보보호위원회** **. 기본 계획 및 시행계획** **. 정책, 제도, 그리고 법령의 개선** **. 공공기관간의 의견 조정** . 법령의 해석 및 운영 . 개인정보 이용, 제공에 관한 사항 . **개인정보영향평가** 관련 . **시정조치 권고**에 관한 사항 . 처리 결과의 공표

개인정보보호감독기구의 독립성은 다음과 같은 **13가지 평가기준**(evaluation criteria)으로 평가될 수 있다.[5)]

5) Graham Greenleaf, Independence and power of data protection authorities: International Standards and Asia-Paciffic Example, Symposium on Analyzing the role and position of an Institution Protecting Individual Privacy, National Human Right Commission of Korea, September, 2009

- 감독기구가 법에 근거해 설립(establishment by law)
- 독립 조사권(independent investigation power)
- 임기보장(fixed term of office)
- 법에 면직조건 명시(removal from office)
- 직무관련 개인소송 저항권 (immunity against personal law suite relating performance of official duties)
- 행정 수반보다는 국회에 의한 임명
- 행정부와 독립적인 행정 및 자원 확보
- 국회에 정기적 보고 의무 및 권한
- 임기종료 후 일정기간 지속 가능 직위 공유 (예, 법원 위원회)
- 독립 감독관의 겸직 금지 및 다수위원회의 이해관계 공개 의무
- 독립 감독관(sole commissioner) 또는 다수 위원으로 구성된 감독기구(multi-member commission)
- 고충처리위원회, 국가인권위원회 등과 같은 위원회와의 기능 통합
- 국가인권위원회 등과 같은 타 기구의 일부 조직

[표 4] 세부 평가기준에 따른 세 후보 법안 비교・평가

	이해훈의원안	변재일의원안	정부안
감독기구의 법 근거 설립	- 만족	- 만족	- 만족
감독관 임기 보장	- 만족 . 3년, 1회 연임 가능	- 만족 . 3년, 1회 연임 가능	- 만족 (위원장, 위원) . 2년, 1회 연임가능
감독관 법 근거 면직	- 만족	- 만족	- 일부 만족 . 대통령령에 위임(추정)
직무관련 개인소송 저항권	- 불만족	- 불만족	- 불만족
국회에 의한 임명	- 불만족 (대통령임명) . 위원장 1인,	- 일부 만족 (입법, 사법, 행정부 수장이 임명)	- 불만족 (국무총리임명) . 위원장 1인과 15명

	이해훈의원안	변재일의원안	정부안
	상임위원 1인 포함 9인의 위원으로 구성 . 위원장은 국무총리 추천으로 대통령이 임명	. 국회:3인, 대법원:3인, 대통령:3인, 위원장은 대통령 임명	이내의 위원으로 구성 . 위원장은 국무총리가 임명
국회 년차 보고 의무	**- 만족**	**- 만족**	**- 불만족**
임기 종료후 일정기간 지속 가능 직위 공유	**- 불만족**	**- 불만족**	**- 불만족**
감독관 겸직금지	**- 만족(추정)**	**- 만족(추정)**	- 해당사항 없음 . 비상임 위원
위원구성	- 다수위원 감독기구	- 다수 위원 감독기구	- 다수위원으로 구성된 위원회(총괄, 분쟁조정)
타 위원회 기능 포함 여부	**- 독립 기능**	**- 독립 기능**	- 해당 사항 없음
타 조직 일부	**- 별도 조직**	**- 별도 조직**	**- 행정부 소속형**

독립성 평가를 위한 세부 평가변수로 분석한 후보 법안에 대한 분석 결과는 [표 4]와 같다.

결론적으로, [표 3], [표 4]의 분석에서 알 수 있듯이, 일반 평가기준과 세부 평가기준을 이용해 평가된 감독기구의 독립성 강도를 살펴보면, **변재일의원안 ≳ 이혜훈의원안 > 정부안** 의 순으로 평가되었다.

제3장 국내 개인정보보호 법제화를 위한 고려사항/추진방향

개인정보보호 감독기구의 독립성 확보가 개인정보보호 법 제정을 위한 가장 중요한 변수중의 하나이나 전부는 아니라고 생각합니다. 또한, 정보주체의 개인정보보호를 완벽하게 보장하기 위해 **독립성이 강한 감독기구를 수립하는 것이** 가능하다고 생각한다.

그러나, 현재 상정중인 개인정보보호법의 제정을 완성하기 위해서는 다음과 같은 국내의 추가적인 **사회·문화·환경적 고려사항**을 염두에 두어야 한다.

- 현재의 개인정보보호 법제화가 부문별 개인정보보호 체계를 보다 개선된 포괄적 형태의 법제도로 향상하기 위한 과정으로 볼 수 있고, 따라서 추진되고 있는 법제정이 **백지 설계(clean slate design)가 아닌 진화 설계(incremental design)** 임을 고려해야 한다.

- 우리나라 경제사회적 환경과 지금까지의 **법적 관행·전통 (practice&tradition)** 등을 고려해야 하며, 동시에 국제표준기구와 주요 외국의 글로벌 수준의 개인정보보호 처리를 보장하고 **아시아·태평양·유럽 등의 주요 외국의 모범 사례(best practice)**를 고려해야 한다.
  . **행정안전부가 공공부분 개인정보보호 기능**을, **방송통신위원회가 정보통신 부문의 개인정보보호 기능**을, 그 외 타 정부부처가 개별 분야의 개인정보보호 기능을 책임지고 있음.

- 현재 한국의 이명박정부는 기본적으로 **작고 효율적인 정부 형태**를 지향하고 있고 비즈니스 친화적인 정책을 기반으로 하는 **규제 완화**에 집중하고 있다.

- 정부 내에 다수 위원회를 설치함으로써, **정부 조직 간의 마찰의 소지를** 없애는 감독기구 체계 수립도 고려해야 한다는 견해도 타당성이 있다. 또한 비용효과를 고려하면 국가 인권위원회와 같은 기능이 **유사한 기능을 갖는 위원회에 개인정보감독기능을 통합하는 것도** 가능하나 현재 3가지 후보법안에는 고려하고 있지 않고 있다.

- 행정안전부가 업무 특성상 개인정보 침해 가능성이 크므로 행정안전부도 감독대상기관이라는 점에서 감독대상기관이 감독기관의 역할을 겸한다는 것은 **객관성, 공정성, 투명성 측면에서 문제가 있다는 지적**도 고려해야 한다. 다만, 이러한 문제는 년차 보고서를 통한 **국회의 감시 및 견제**, 감사원의 **감사** 및 부처의 자체 감사를 통해서도 일정부분 보완할 수도 있다고 생각합니다.

- **정부부처로부터 독립적인 개인정보보호 감독기구의 설치가 개인정보보호를 달성하기 위한 필요 충분·조건이 아니라는 견해**도 타당하며, **행정부 소속형의 개인정보보호 추진체계가 채택**되더라도 개인정보보호위원회의 **권한 강화와 위원 구성의 독립성 제고 등의 실질적인 기능상의 독립성을 강화하는 방안 마련도 장기 과제**로 고려할 필요가 있다. 이 경우, 행정안전부 산하에 개인정보보호만을 전담하는 개인정보보호위원회를 설치하는 방안도 고려할 필요가 있다.

제4장 결론

기존의 개별·분산 형태의 개인정보보호 법체계의 문제점을 해결하기 위한 포괄적 형태의 **개인정보보호법 제정은 국민적 합의**를 이미 얻었다고 생각하며, 매우 **시급한 현안(pending issue)이라고** 생각합니다. 법제정을 위한 지금까지 노력과 합의를 근거로 **입법자간의 조속한 합의와 타협이 필요한 때** 라고 생각합니다. 오늘 심포지움에서 제시된 발표가 국내에서 **조속한 개인정보보호 법 제정을 위한 전기를 마련**하고, 오늘의 토론의 결과가 **이를 위한 긍정적인 영향**을 주기 희망합니다. 이번 기회를 빌어 상당한 수준의 국민적 합의에 도달한 개인정보보보법 제정이 금년 이내로 완성될 수 있기를 바라면서 발표를 마칩니다. 마지막으로 탁월한 주제 발표를 해주신 Marie GEORGES 자문관과 G.Greenleaf 교수님께 감사의 말씀을 드립니다.

개인정보감독기구의 설립을 둘러싼 쟁점과 방향설정

이인호 (중앙대학교 법학전문대학원 교수)

2
토 론

The Issues Concerning Establishment of a Data Protection Authority and the Orientations for its Establishment and Operation

Inho Lee (Prof. Dr, School of Law Chung-Ang University)

Contents

I. Introduction

In Korea, the Government, civic organizations and the academia have made consistent and multilateral efforts to streamline the existing complicated system of personal data protection since 2003. As there exist a variety of individual laws on personal data protection and they are divided over the public and private sector, both the data processing agencies and the general public (data subjects) have an insufficient understanding about those laws, which has undermined their effectiveness. Another problem is that there is no general law for data

protection in the private sector, leaving some private activities outside the legal regulation and protection. In an effort to address these problems, there have been some movements to enact a general law governing the personal data processing in both the public and private sector, and these movements have recently evolved into the three draft bills on personal information protection: the bill proposed by Parliamentarian Hye-hoon Lee, the one by Parliamentarian Jae-il Byun and the one by the Government, which are all under review by the Parliamentary Committee on Public Administration and Security as of September 2009.

With regard to the enactment of a general comprehensive law on personal information protection, there exist very conflicting opinions on several issues. Those hot issues can be grouped into three categories: the first is about the legislative system - how the different individual laws governing the different areas of activities could be systematically coordinated?; the second concerns a substantial issue - what are the enforceable standards for personal data processing (collection, use and disclosure) which harmonize the values of use and protection in a reasonable and balanced way? (the criteria for approval of personal data processing, procedural requirements of the processing and the right of data subjects to participate are included); and the third is about the enforcement structure - how are those standards enforced, especially including how is the DPA organized and what powers and functions are provided for the DPA?

This symposium hosted by the National Human Rights Commission of Korea under the title "Analyzing the Role and Position of an Institution Protecting Individual Privacy" will focus on the third issue, that is, the enforcement structure. I am greatly pleased to have an opportunity to share the valuable experiences and expertise of the two presenters, Professor Graham Greenleaf from Australia and Ms. Marie Georges from France, who are the internationally recognized authorities in this field. I hope that their experiences and expertise will give us a precious clue in addressing the challenge facing this country.

The three bills now pending the Parliament are all about a general law covering both the public and private sector. They specify legal standards for fair data processing (collection, use, disclosure, etc.) applicable to all the agencies which process personal information in the form of searchable database (including manual files) ("personal information processing agencies") and provide for an authority which enforces or supervises compliance with the standards. In other words, the common purpose of the bills is to allow an adequate use of personal information, while creating safeguards to protect the rights and interests, including privacy, of data subjects.

In fact, the 'Personal Information Protection Act' envisioned in the bills is not a privacy protection law.[1] It means that the 'Act' is not intended simply to "protect" personal information but also to promote "safe use" of personal information. The underlying objective of the 'Act' is to facilitate the use of personal information which is required in the society by establishing safeguards and protections to prevent the risks involved in an indiscreet use of personal data (such as violations of data subjects' privacy and damages due to ID stealing). It is true that the use and distribution of personal information is a must for normal functioning of this complicated modern society, but if personal information is used indiscreetly without safeguards, it will make the general public feel more unsecured and undermine the necessary flow of personal data. Accordingly, the first thing to do to ensure an adequate use and flow of the personal information which is required for proper functioning of the society, is to set up safeguards to prevent personal information from being used indiscreetly.

One of the safeguards is an "independent supervisory body for personal data protection". The reason why 'independence' is a critical element of such body is that the personal data processing agencies subject to the supervision of the body are the Government agencies.

1) Inho Lee “Understanding of the Personal Information Protection Act as a privacy protection law of the second generation", *Sabup*(Law) Vol. 8 (Judicial Development Foundation, June 2009) pp. 36-85

Although private companies have a great amount of personal information databases for the purpose of business operation in recent years, it is the Government agencies that have a long tradition of creating and processing the databases of personal information to perform their responsibilities.[2] Therefore, the Government agencies constitute a large majority of the organizations that are governed by a personal data protection law and are supervised by a DPA. Understandably, the supervisor and those under supervision should be separated in their functions, and the supervising agency should be independent of the agencies subject to supervision so that the former can perform independent activities of supervision.

The critical element here is the "functional independence". The independence of a DPA means its functional independence, rather than a complete separation in terms of organizational structure. Accordingly, we cannot say that a DPA is not independent just because it is placed under the President or the Prime Minister.

For this reason, the three bills which were submitted to the 17th Parliament and were later automatically cancelled proposed that, in order to ensure independence of a DPA, it should be under the Prime Minister or be an independent body like the National Human Rights Commission of Korea (NHRCK). However, the Ministry of Public Administration and Security (MoPAS), in the first public hearing of June 27 this year, revealed a draft bill providing that MoPAS shall be a responsible ministry to supervise the enforcement of the 'Personal Information Protection Act' and the Personal Information Dispute Mediation Committee shall be set up under MoPAS for a limited function of dispute mediation.[3] This publication was greeted with criticism from some civic groups, including *Jinbo Net*, and commentators that the Government bill excluded the independent nature of a DPA. In

2) As of 2006, the number of personal information databases ("personal information files") held by public agencies was 1,144: which is broken into 277 by national administrative agencies; 397 by local governments; 67 by educational institutions; and 403 by state-invested agencies. See Ministry of Public Administration and Security, *The List of Personal Information Files held by Public Agencies*, 2006.

3) Ministry of Public Administration and Security, The Documents for Public Hearing on Legislation of 'Personal Information Protection Act', June 27, 2008.

response, MoPAS included some amendments in the bill and made an official notice about the draft bill on the Personal Information Protection Act on August 12. The Government bill was published in the 2nd public hearing of August 28 and is now pending the Parliament.

The Government bill provides that MoPAS shall responsible for enforcing the Act and supervising compliance with the Act; the Personal Information Dispute Mediation Committee shall perform the function of mediating relevant disputes; and a new Personal Information Protection Commission shall be created under the Prime Minister to deliberate some defined matters. It is questionable whether the new Commission as is defined in the Government bill can be viewed as a DPA and whether the structure of enforcement and supervision included in the bill can guarantee independent supervision.

II. Rationale for a specialized and independent DPA

(ⅰ) The problem involved in the law enforcement in relation to personal information processing may arise from the fact that personal information is extensively collected, accumulated, processed, disclosed or shared by the Government or private companies, with the data subjects not knowing about such activities. It is unlikely that the data subjects, being unaware that their personal information has been infringed, will initiate a process of remedies.

(ⅱ) Even if the collection limitation principle and the system openness principle, two of the principles for personal information processing, are fully respected and the data subjects are well informed about the collection and processing of their personal data, they cannot gain an sufficient understanding about the possible breaches within the processing agencies, nor can they make investigations into the internal process. The data subjects, usually not specialized in the technically complex process, cannot check if their personal information is not used or disclosed for other purposes than are consented.

(iii) Furthermore, even when the data subjects detect any breach by the processing agency, it is not easy at all for them to initiate and go through a long and complicated course of filing a complaint for remedies before the court. Given that the remedies given by the proceedings in the Court is just an ex post facto solution, it is imperative to ensure preventative remedies for the personal information rights.

(iv) In general, the processing of personal information databases involves a large number of individuals, not about some particular individuals, and so any unlawful processing of personal data has an equal harmful impact on all of the individuals involved. That is to say, the damage from unlawful data processing is of extensive and collective nature.

(v) There is a strong need to ensure that the DPA governing the public sector perform its functions independent of the Government. The value of personal data protection is always at odds with the efficiency value that can be obtained from the data processing.

In order to substantially protect individuals' right to self-determination of personal data from unlawful data processing by the Government and private companies, it is necessary to establish an independent DPA which monitors and supervise personal data processing in a preventative and proactive manner and, in the event of a violation, allows the affected individuals to access a more effective and efficient channel for remedies than the proceedings before the court.

The need of an independent DPA has been confirmed by some world-renown analysts in the field of personal information protection. Mr. Colin J. Bennett, Professor at the University of Victoria, Canada and Mr. Charles D. Raab, Professor at the University of Edinburge, the UK once said, "The presence of a strong supervisory body has been considered *sine qua non* of a good system for privacy protection. For a law cannot be enforced by itself and the privacy culture cannot be established by itself without influential advocates."[4)]

In addition, Mr. David Flaherty, the former Personal Information Protection Commissioner of the British Columbia State in Canada asserted that "a DPA is kind of an alarm system for the protection of privacy."[5)]

To sum up, creating an independent DPA is no longer a matter of choice. Korea, as an OECD member state and the world's 12th largest trading nation, needs to be committed to international standards and, as an IP powerhouse, must create an independent DPA to lay the groundwork for a highly information-based society where human dignity is fully respected.

Many nations in the world are moving towards a single DPA combining both the private and public sector, under the strong influence of the European Union Directive on Personal Information Protection (95/46/EC). This trend is not confined to the member states of EU and Council of Europe (CoE), but is also found among the non-member states. Tables 1 and 2 below show a list of countries with such DPA:[6)]

4) Colin J. Bennett & Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Ashgate, 2003), p. 107.

5) David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (1989), p. 383.

6) The Tables summarize the data from the Website of the Council of Europe. <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Supervisory_authorities/>

Table 1. DPAs in CoE member states

Country	DPA	Website	Country	DPA	Website
Austria	Büro der Daten-schutzkommission	www.dsk.gv.at	Luxembourg	Commission nationale de la protection des données	www.cnpd.lu
Belgium	Commission de la Protection de la vie privée	www.privacy.fgov.be	Netherlands	College Bescherming Persoonsgegevens	www.dutchdpa.nl
Bulgaria	Personal Data Protection Commission	www.cpdp.bg	Norway	Datatylsinet	www.datatilsynet.no
Croatia	Personal Data Protection Agency	www.azop.hr	Poland	Bureau of Inspector General for Personal Data Protection	www.giodo.gov.pl
Cyprus	Office of Personal Data Protection Commissioner	www.dataprotection.gov .cy	Portugal	Commissão Nacional de Protecção de Dados	www.cnpd.pt
Czech Republic	Office for Personal Data Protection	www.uoou.cz	Rumania	National Supervisory Authority for Personal Data Processing	www.dataprotection.ro
Denmark	Datatilsynet	www.datatilsynet.dk	Slovakia	Commissioner For Personal Data Protection	www.dataprotection.gov. sk
Finland	Office of Data Protection Ombudsman	www.tietosuoja.fi	Slovenia	Information Commissioner	www.ip-rs.si
France	Commission Nationale de l'Informatique et des Libertés	www.cnil.fr	Spain	Agencia Española de Protección de Datos	www.agpd.es
Germany	Bundesbeauftragte für den Datenschutz	www.datenschutz.de	Sweden	Datainspektionen	www.datainspektionen.se
Greece	Data Protection Commission	www.dpa.gr	Switzerland	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragt er	www.edoeb.admin.ch
Hungary	Data Protection Commissioner	www.obh.hu	UK	Office of the Information Commissioner	www.ico.gov.uk
Iceland	Persónuvernd (Data Processing Authority)	www.personuvernd.is	Italy	Garante per la protezione dei dati personali	www.garanteprivacy.it
Ireland	Data Protection Commissioner	www.dataprivacy.ie	Estonia	Inspection of Data Protection	www.dp.gov.ee

Table 2. DPAs in non-member states

Country	DPA	Website	Country	DPA	Website
Canada	Privacy Commissioner	www.privcom.gc.ca	Australia	Privacy Commissioner	www.privacy.gov.au
Hongkong SAR	Office of the Privacy Commissioner for Persona Data	www.pco.org.hk	Monaco	Commission de contrôle des informations nominatives	www.ccin.mc
New Zealand	Privacy Commissioner	www.privacy.org.nz	Thailand	Official Information Commission's Office	www.oic.thaigov.go.th

III. Functions and powers of DPAs

The DPAs in the world serve as one of more of the seven interrelated roles: i) ombudsman; ii) auditor; iii) consultant; iv) educator; v) negotiator; vi) policy advisor; and vii) enforcer.

Certainly, it is not that all DPAs place an equal emphasis on all of those roles, and these roles are not exclusively played by DPAs. In some countries, the government ministries have an important role to play in protecting personal information. The following gives a more detailed description on those roles and functions.[7)]

1. DPA as an ombudsman

First, all DPAs perform the function of receiving complaints from data subjects, investigating into factual aspects and resolve the complaints. This traditional 'ombudsman' function of "receiving, investigating and resolving complaints" is a core element for efficient supervision by the regime of personal data protection, although it requires a large amount of time and resources.

7) This description is largely based on Colin J. Bennett & Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Ashgate, 2003), pp. 109-114.

In creating a system to handle complaints, it is crucial to make a thorough review on which powers should be given to the DPA to ensure the ombudsman function is properly performed. Although it may differ from country to country, the related DPA powers usually include: i) the power to enter the premise of data processing agencies; ii) the power to demand the relevant records resulting from the personal data processing; and iii) the power to call the person(s) responsible for the data processing. One difficult question in this regard is whether the DPA may exercise the power to investigate alleged violations on its own initiative, even without any complaint by data subjects. Some countries provide for the DPA's power to investigate by authority.

Meanwhile, complaint resolution can be made in various ways: for instance, by binding enforcement orders in the UK or by less mandatory recommendations in Canada, New Zealand and Australia. The DPAs which heavily depend on the methods of conciliation and mediation should make good use of the tendency of data processing agencies to be eager to reach conciliation with the complaints for fear of negative publicity.

2. DPA as an auditor

The work of complaint investigation and settlement is, in nature, passive. However, in case a DPA is suspicious of a particular processing agency for its processing practices, it may conduct a general audit on the agency or particular techniques. Audits are more systematic and less confrontational than the investigations accompanying specific complaints.

The Federal Data Protection Commission of Germany has carried out audits on the personal data processing systems from the initial years.[8] The DPAs in Germany have developed the inspection methods that cover all the aspects of personal data processing within a data processing agency.[9]

8) David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (1989), p. 77.

Audits are classed into several types, depending on how often they are made and how strict they are. For instance, in Canada, an audit programme has been a routine activity of the Federal Privacy Commission although it is not specified in the federal Privacy Act. In some Canadian States, site visits, as a less official method, may be made. Mr. David Flaherty, when he was the Personal Information Protection Commissioner of the British Columbia State, encouraged informal site visits to large public agencies.[10)]

On the other hand, the data protection laws in some countries expressly provide for the auditing function of DPAs. For instance, the Personal Information Protection and Electronic Documents Act, which is a federal law to protect personal information in the private sector, envisages that the audit function may be delegated to the Personal Data Protection Commission, an accounting firm or a standard certifying agency at the level of states. In the Netherlands, the national Commissioner may require, in certain conditions, that audits should be conducted by a publicly certified auditing agency.

3. DPA as an consultant

Every DPA provides advice and consultation to individual processing agencies on how they can observe the provisions of the personal information protection law. It is not exaggerating to say that implementation of the personal information protection law largely depends on how faithfully the DPA performs its advisory function, whether it has a strong statutory power or not. It is the most important to encourage and advise data processing agencies to equip themselves with a personal data protection system in advance, instead of exercising a compelling power *ex post facto*. Advice and consultation is regarded as being much better than the confrontational relationship between the regulator and those regulated, which might

9) Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press, 1992), p. 182.

10) See David H. Flaherty, "How to Do a Privacy and Freedom of Information Act Site Visit" <http://www.oipcbc.org/>.

need a high cost and be inefficient.

In particular, in the cases where such new techniques or systems as may violate privacy are adopted, the role of the DPA as a consultant is of great significance. In general, data processing agencies want to know in advance whether a new system which they plan to adopt is in compliance with the personal data protection law. The tendency is that this advisory function is frequently performed outside formal procedures, and the DPA must be careful in giving advice and consultation in an impartial and prudent manner, without prejudice to its independence, lest a complaint should be made to data processing agency at a later time.

4. DPA as an educator

Apart from advice and consultation for individual processing agencies, a DPA performs a broader function of education and studies. It is very important to analyze and study the issues of surveillance and privacy in a broader context and continue to educate data processing agencies and data subjects, promoting a culture of privacy protection within the government and throughout the society. All of the DPAs in the world have this function, although its coverage and intensity is greatly different among different DPAs.

A DPA needs to focus its resources, although limited, on increasing people's awareness towards the ideas and principles of personal data protection and promoting the privacy protection culture. Some interesting examples are found among the DPAs in the world.

For example, the Office of the Privacy Commissioner of Canada has published a "Guide for Businesses and Organizations" with a view to informing the general public accurately of the contents of the 'Personal Information Protection and Electronic Documents Act' which is a general law for the private sector.[11] This Guide, in an effort to ensure compliance with the

11) For more details of the Guide, see <http://www.privcom.gc.ca/information/guide_e.asp>.

law provisions, gives a detailed explanation about the scope of regulation, the principles of fair data processing and the remedies for rights violations in plain language. The Office also provides such information as could help private companies comply with the law provisions.[12] Another example is the "Privacy Diagnostic Tool" in the Canadian State of Ontario. This Tool has been developed jointly by the State Office of Information and Privacy Protection and major accounting companies, in a bid to help data processing agencies make a self-diagnosis or self-assessment on whether they are in compliance with the principles of personal information protection.[13]

Many other DPAs have made great efforts to devise a similar self-diagnosis program. For instance, the Office of Privacy Commissioner for Personal Data (PCO) of Hong Kong developed and released "Privacy.SAFE: Guidance Notes for Self-Assessment" in 2002 to assist the personal data processing agencies of the public and the private sector in self-evaluating their compliance with the Personal Data [Privacy] Ordinance.

As are seen above, DPAs study the privacy problems involved in particular areas or technologies, seek after solutions to the problems and sometimes conduct an opinion poll. The reports based on the research results are used as a valuable means to warn the government, private companies and individuals against the privacy risks inherent in the new technical innovations.

5. DPA as a policy adviser

Generally, the Personal Information Protection Act requires the DPA to make comments or give advice on what implication a new bill has about privacy protection and what impact a new automated personal data system will have on privacy protection. For instance, the Privacy Act of Canada entitles the federal Office of the Privacy Commissioner to make a

12) The information resources are included in <http://www.privcom.gc.ca/ekit/ekit_e.asp>.
13) For more details of the “Privacy Diagnostic Tool”, see <http://www.privcom.gc.ca/ekit/ct_01_e.asp>.

special report to the Parliament on such particular issues as are within its jurisdiction.[14]

As is often the case in many nations, the Office of Privacy Commissioner of Canada is always in conflict with the federal government while they are in the census process.[15] In the UK, when the government proposed an extensive data-sharing project to expand the government's public service and prevent fraudulent practices, the Personal Information Protection Commissioner gave policy advice on what effect the government's proposal would have on privacy protection.[16] In some other countries, whenever a government agency introduces a new technological application, it is required to prepare a "privacy impact statement".[17]

Additionally, DPAs give testimony in a Parliamentary hearing on a relevant issue or make an official objection to a particular government policy. In a widely known example of an official objection, in 1995 when the Home Office of the UK announced a plan to introduce an ID card system, the UK Registar (what is now Information Commissioner) expressed a grave concern about its impact. At the time, the UK Registar conducted its own survey of the public opinion on the system and published the survey results.

6. DPA as a negotiator

The DPAs in some nations have an explicit obligation to negotiate a privacy code of

14) Privacy Act, Sec. 39(1).

15) See Canada, Office of the Privacy Commissioner (OPC), Annual Report 1999-2000 (Minister of Public Works and Government Services Canada, Ottawa, 2000), pp. 49-52 .

16) See United Kingdom, Performance and Innovation Unit, Cabinet Office, Privacy and Data-Sharing: The Way Forward for Public Services (Cabinet Office, 2002). <http://www.number-10.gov.uk/su/privacy/downloads/piu-data.pdf>

17) For details on the privacy impact statement system of the US and Canada, see Byung-Moon, Gu, "The initiatives to incorporate the privacy impact statement system in the domestic law - expecially for the public sector", The 3rd Personal Information Protection Policy Forum (Government Reform and Decentralization Commission, June 16, 2004), pp. 38-46; Gyu-Jeong Lee and Byung-Moon Gu, *The Privacy Impact Statement System in the Public Sector*, (National Computerization Agency, 2003).

practice as a self-regulatory norm of private organizations.

The privacy code of practice for self-regulation has clear strengths even when there exists a national law on personal information protection. In the course of negotiating a privacy code of practice, the private organization concerned and the DPA can increase mutual understanding about the privacy matters. The code of practice is a very flexible norm which is easily adaptable to the changing economic conditions and technological innovations. In addition, as a personal information processing agency publishes its privacy policy in the code of practice, the code can help remove any suspicion about the processing practices of the agency. In brief, the privacy code of practice may make substantial contribution to increasing mutual understanding between the DPA and data processing agencies.

However, it is very difficult to define the relationship between the self-regulatory code of practice and the national law on personal information protection. An analysis on the experiences of the nations where the privacy code of conduct has been utilized and promoted reveals three different models that are slightly different from each other.

First is the strictest one which has been adopted in the Privacy Act of New Zealand. [18] The core element of the New Zealand-style model is that the privacy code of practice, once it is established in accordance with the Privacy Act, has a force of law. Accordingly, a breach of the approved privacy code of conduct shall be treated as a breach of the personal information protection principles in the Privacy Act, and consequently, invoke the procedures of complaint handling and enforcement as are provided in the Act.

Second is a relatively flexible model of the Netherlands. This model is similar to the one of New Zealand in many respects and also involves a process of prudent negotiation over the code. However, in this model, the code has no binding force towards the court. Of course, in

18) New Zealand Privacy Act 1993, Secs. 46-53.

case a particular processing agency can prove its compliance with the requirements in the code, the proof may be a good defense for the agency. However, if the complainant proves that the agency has violated the rules of the code, that would be the *prima facie evidence* which imposes a liability under the Act. In this way, the privacy code of practice has an indirect, if not direct, force of law.

The third model is found in the UK and Canada and, in this model, the personal information protection law simply entitles the DPA to encourage the creation of a privacy code of practice. Here, the code does not have even an indirect force of law. As a matter of fact, this model is envisioned in Article 27 of the EU Directive (95/46/EC).

It seems that there exists a dilemma in utilizing the self-regulatory privacy code of practice in the jurisdiction with a comprehensive law protecting personal information. If the code of practice is not subject to approval from the DPA, it may contain such rules as are contradictory to the provisions of the law, making it more difficult to apply and enforce the law. On the other hand, however, if there is an official procedure to gain the DPA's approval, the original intention for the code as a flexible self-regulatory norm would be deleted and the code has a risk of being bureaucratized.

7. DPA as an enforcer

It is an important question whether a DPA should be given the power to order directly the data processing agencies to implement the personal information protection principles. This executive power, which enables the DPA to make a direct order for rectification of inappropriate actions, should be distinguished from the function of investigation or recommendation.

Some commentators argue that more emphasis should be placed on the advisory function

than on the function as an enforcer. They also believe that, in case a data processing agency seems to be unfaithful in protecting personal information, just revealing such unfaithfulness to the general public would be a very effective sanction against the agency.

On the other hand, however, some other commentators argue that even when the executive power is rarely exercised, the presence of the power itself has an effect of inducing the processing agencies to comply with the law. Moreover, the data processing agencies in the public and the private sector need to retain certainty and coherence in applying the principles of personal information protection. Over time, the procedures of exercising a formal power of enforcement would guarantee a much higher degree of coherence, transparency and accountability in the course of law application. Then, the proportion of law conformity will grow with time.

In most nations, the personal information protection law provide that the final remedies for rights violations should be given in the court and that the complaint settlement procedure under the DPA may be reviewed by the court. Meanwhile, some nations, in the belief that a court is not always the best institution to handle comparatively professional and technical disputes, have set up a tribunal which is composed of a small number of specialists and performs a quasi-judicial function. For instance, the 1998 Data Protection Act of the UK provides for establishment of the Data Protection Tribunal and specifies that in case an individual or a data processing agency finds the decision by the Information Commissioner unsatisfactory, he/she/it may file a protest to the Tribunal. If necessary, the Tribunal may be set up as a panel of experts.

IV. Directions for establishment of the DPA in Korea

In general, the DPA is not a traditional administrative agency with the executive power. Nor does it need to be an agency making decisions about the information policies at the national level.[19)]

The aforementioned functions of the DPA are grouped into three broader categories: **prevention, complaint settlement *ex post facto*** and **policy advice**. First, the function of prevention is to induce the data processing agencies to conform to the substantive provisions of the data protection law (that is, the obligatory provisions based on the principles of personal information protection) in advance in order to prevent any inappropriate processing of personal data. The functions of auditing, consultation, education and negotiation for self-regulation belong to this category.

Second is the function of *ex post facto* complaint settlement. That is, DPAs receive complaints from data subjects, investigate into factual aspects and settle the complaint. This traditional 'ombudsman' function of "receiving, investigating and resolving complaints" is a core element for efficient supervision by the regime of personal data protection. Certainly, the method of complaint settlement varies, depending on the type of violation. DPAs may lead the disputing parties into conciliation; initiate a mediation process when a damage has occurred; file a suit to the court on behalf of the complainant; ask for prosecution in the event of such serious offence as is subject to a criminal penalty; or recommend a competent authority to impose an administrative sanction (discipline or monetary penalty).

Thirdly, a DPA may serve as a policy advisor. While the functions of determining and

19) Professor Il-hwan Kim argued that "it is neither legitimate nor adequate that a supervisory body makes decisions about information policies instead of the Parliament or the Executive on the ground of the lack of their democratic legitimacy." Il-hwan Kim, "The study on how the personal information protection legislation should be streamlined", (Korea Legislation Research Institution, 1997), p. 198.

enacting policies are left to the Parliament and the Executive, the DPA may and should provide advice in the policy-making process.

The future DPA of Korea should be able to perform all of the three broader functions and should be given the powers required to perform them. Additionally, sufficient independence should be guaranteed in terms of the organizational structure and budget allocation.

Still, whether the new DPA should be given the executive power needs to be thoroughly reviewed, in the light of the particular reality in Korea. The executive power would enable the DPA to order directly the data processing agencies to rectify their practices to conform to the law provisions. For instance, in case a data processing agency is found to have processed personal information in contravention of the provisions of the data protection law (into which the principles of personal information protection are embodied), the DPA could order the agency to suspend its work of data processing or to discontinue the operation of its data processing system. It also could exercise some sanctions, including monetary penalty, if the agency fails to implement the enforcement order. The DPA with this executive power would have some features of a traditional administrative authority, and it would look like, for example, the Fair Trade Commission or the Korea Communications Commission as they are.

However, considering that the DPA would supervise the public sector, as well as the private sector, it is somewhat questionable if it could exercise a strong executive power over the public sector effectively enough. In my judgment, a direct order is not the only way to correct the breaches in public agencies. There are many indirect but effective methods. For example, publishing the violations, reporting them to the Parliament or a higher-level supervisory body and leading the public opinion are some of the effective methods to correct the breaches in public agencies.

Accordingly, it is believed that the new DPA needs to be a supervisory body in such form

as can minimize the tension with the existing institutions and agencies, instead of being given the executive power from the beginning. What should be done first at this time and in this situation is to concentrate on activating and institutionalizing the three fundamental functions of prevention, complaint settlement *ex post facto* and policy advice, so that the DPA can exercise its potential to the maximum and evolve into an effective system of personal information protection.

The presence of an independent DPA does not automatically lead to an effective system of personal information protection. The DPA, with limited physical and human resources, cannot perform supervisory work for each and every data processing agency. For this reason, it is necessary to ensure that every data processing agency, whether in the public or private sector, designates a Chief Privacy Official (CPO) with an independent status and role within the agency. It is very important and critical that the CPO serves as a primary supervisor who monitors the personal data processing in the agency and ensures conformity to the personal information protection law. The COP, while being part of the particular agency, is a site auditor from the DPA in functional terms.

V. Assessment of the enforcement structure in the Government bill

1. The existing enforcement structure and its limitations

It is necessary and urgent to create a specialized and independent DPA which supervises and enforces the compliance with the personal information protection principles in the private and public sector in an effective and coherent manner and promotes effective remedies to rights violations. In this regard, the existing organizations for personal information protection in Korea have some limitations.

(1) First, as there exist **different individual bodies for different sectors** and there is no comprehensive system for personal information, many areas of activities are left outside the legal protection. Apart from the work of the Privacy Violation Complaints Center and the Commissioner for the Mediation of Conflict on Personal Information (CMCPI), both of which were set up under the former Ministry of Information and Communications (now, under the MoPAS and the Korea Communications Commission), it is not exaggerating to say that the other organizations have done almost nothing. As is seen in the National Education Information System (NEIS) case of 2002 and 2003,[20] the then Ministry of Government Administration and Home Affairs, which was a responsible ministry under the "Public Agency Data Protection Act" and the Personal Information Protection Commission had done nothing to protect personal information in the course of the establishment of the data processing system.[21]

In a broader definition, a DPA includes an organization which, although not being expressly specified as such in the law, performs a protective function in practice, and Tables 1 and 2 below are the lists of the DPAs now in operation in Korea.

20) The National Education Information System (NEIS) was a nationwide information system integrating all the data for educational administration, including the personal data of the primary and secondary school students, which had been built up by the then Ministry of Education and Human Resources Development in 2001 with no legal foundation.

21) According to the data released in 2003 by the People's Solidarity for Participatory Democracy based on the document it had received from the Ministry of Government Administration and Home Affairs about the activities of the Personal Information Protection Commission, there were three meetings during the five years from 1998 to 2002 and two of them were in the form of paper review. That is, there was only one formal meeting during the five years.

Table 1. DPAs for the public sector

DPA	Applicable law	Coverage	Main function	Features
Minister of Public Administration and Security	Public Agency Data Protection Act	Personal data held by public agencies	· Prior consultation/publication of the personal information DB held by public agencies · Request for documents and fact-finding investigations · Receipt of complaints on violations, verification of factual aspects, notification of the results and notification to the complainant · Advice and recommendation to public agencies	· Administrative authority (independent entity) · Non- specialization /non-independence · Responsible for the e-government project
Personal Information Protection (Public Agencies) Commission	Same as above	Same as above	· Review for policy and institutional improvement · Review of the coordinated opinions of public agencies about use and disclosure of personal data · Review of the matters at the request of the Minister of Public Administration and Security · Review the issues involving use and disclosure of personal data for other purposes	· Under the Prime Minister (Chaired by Minister of MoPAS) · Review board · Non- specialization /non-independence
Minister of Education, science and Technology / Educational Superintendents	Primary and Secondary Education Act	Educational data	· Supervision, when necessary	· Creator/ operator of the education information system
National Human Rights Commission of Korea	NHRCK Act	General violations of human rights	· Research and studies on laws/institutions/policies/practices and recommendation for improvement or expression of its opinions · Investigation into alleged human rights violations/discriminations, and remedies for violations · Investigation/education/publicity of human rights conditions · Submission/recommendation of guidelines	· Body to protect general human rights · Independence /non-specialization · Recent reinforcement of the functions of investigating information-related human rights violations /giving remedies

Table 2. DPAs for the private sector

DPA	Applicable law	Coverage	Main functions	Features
Korea Communica-tions Commission (KCC)	Act on the Promotion of the Information Communications Network Use and the Information Protection (AICN)	Personal information of the users of the services provided by the information/ communications service providers	· Investigation into alleged violations (by requesting documents/conducting site inspections) · Order to rectify violations · Imposition/collection of fines · Imposition/collection of other monetary penalties · Development/distribution of personal data protection techniques	· Policy-making and executive agency in the sector of broadcasting/ communications · Presidential independent regulatory commission · Non-specialization (personal information) · Policy/executive power duplication with Minister of MoPAS · Combining policy making and enforcement for the promotion of information/communicati ons network use and the personal data protection
	Act on the Protection, Use, etc. of Location Information (ALI)	Location information	· Accrediting location information businesses · Receiving complaints on the location data-based services · Imposition/collection of fines · Imposition/collection of other monetary penalties · Awarding arbitration on disputes	· Combining policy making and enforcement for the use and protection of location information
Minister of MoPAS	AICN	Personal information of the users of the services provided by (some of) the offline service providers	· Investigation into alleged violations (by requesting documents/ conducting site inspections) · Order to rectify violations · Imposition/collection of other monetary penalties than fines · Development/distribution of personal data protection techniques	· Administrative authority (independent entity) · Non-specialization /non-independence · Policy/executive power duplication with KCC protection
Privacy Violation Complaints Center	AICN	Personal information as defined in AICN	· Counselling and grievance handling (investigating alleged violations/ requesting related documents) · Education/publicity/research · Technical advice/assistance	· Under the Korea Internet & Security Agency (KISA) · Supplementary to the law enforcing work in MoPAS and KCC

DPA	Applicable law	Coverage	Main functions	Features
Commission for Mediation of Disputes on Personal Information	AICN / ALI	Personal information as defined in AICN/ALI	・Receiving applications for dispute mediation ・Investigating factual aspects/recommending an agreement between parties ・Mediation (hearing the parties/ collecting evidence/experts' advice/mediation decision)	・Under MoPAS (members are appointed by the Minister of MoPAS) ・10 members, including 1 permanent member ・Less specialized
Financial Services Commission	Act on the Use and Protection of Credit Information	Credit information	・Accrediting/licensing/ registrating credit information businesses ・Setting the standards for credit information processing ・Counselling and remedies ・Recommendation and order to rectify breaches ・Imposition/collection of other monetary penalties than fines	・National administrative authority under Prime Minister ・Supervising and coordinating financial policies ・Combining policy-making and enforcement for the use and protection of credit information ・Korea Financial Intelligence Unit as a subsidiary to use and report particular financial transactions information ・Cannot be seen as a DPA

(2) Secondly, the existing organizations are very vulnerable in terms of independence and specialization. At present, the responsible authority for personal information protection in public sector is the Minister of Public Administration and Security, who is, at the same time, the head of the Ministry which is responsible for the Electronic Government initiative. For the purpose of an efficient operation of the e-Government, the Ministry will be tempted to put the value of using personal information before its protection. It is very difficult, although not impossible, for the same institution to seek after two conflicting values and try to harmonize them. The Ministry is bound to be inclined to one side.

Meanwhile, the enforcement structure of personal information protection in private sector is

very confusing and insufficient in independence and specialization. With the President Lee's Administration taking office, the Ministry of Information and Communications was abolished and the policy-making and enforcement functions under the AICN have been split between the Korea Communications Commission (KCC) and the Minister of Public Administration and Security. The personal data of the users related to the services by information and telecommunications service providers are covered by KCC and the personal data of the users related to the services by some of the other off-line service providers are covered by the Minister. Furthermore, the Commission for Mediation of Disputes on Personal Information, which is to mediate the disputes in both the on-line and off-line sectors, is under the control of the Ministry of Public Administration and Security, and its Secretariat is placed in the Korea Internet & Security Agency (KISA). The Privacy Violation Complaints Center, which is part of KISA, is functioning as a subsidiary organ for enforcement by KCC and the Minister. This is a very weird structure of enforcement.

As for the on-line service sector, the functions of making and enforcing policies in relation to personal information protection are performed by KCC, which could be much more neutral and independent in protecting personal information than the now-defunct Ministry of Information and Communications (MIC). As the primary responsibilities of MIC were to establish the infrastructure of information and communications and promote the industry of information and communications, it was somewhat difficult for the Ministry to coordinate and balance the conflicting values involved in the use and the protection of personal information. Ironically, as MIC was very sensitive to the public opinion, as is ordinary for an administrative authority, it led the efforts to enact a very strict law overemphasizing the value of information protection and concentrated on the function of *ex post facto* execution and punishment rather than on the function of proactive and preventative supervision. The consequence is that the value of use of on-line personal information died out. The reason might be the lack of specialization. The work involved in personal information protection requires the professional expertise and knowledge on how to strike a delicate balance between the use and the protection of personal information. But MIC, whose staff is always in rotation, could not secure such

professionalism. KCC is suffering a similar difficulty: even though it has secured neutrality and independence, it is not designed specifically for the activities of personal information protection.

(3) Thirdly, all of the existing DPAs are very limited in their functions and roles. Even in the area of information and telecommunications where the protection is the strongest, the functions are limited to: receiving an application for remedies from the data subject, investigating into factual aspects, imposing an administrative sanction (monetary penalty) or reporting the violation to the prosecution, or mediating for civil damages. They have failed to perform preventative and proactive monitoring, coordinate self-regulation or guarantee remedies for collective and extensive violations. In particular, as for the credit information and financial transactions information, the law provides that the Financial Services Commission (FSC) shall perform a given supervisory function, but FSC has not performed the function successfully because it is not designed specifically for that purpose (therefore, is not specialized enough) and it is also responsible for making policies on the use of the credit information and financial transactions information.

2. The enforcement structure in the 3 bills pending the Parliament

Govern–ment bill	· MoPAS Minister shall be comprehensively responsible for policy-making/enforcement/supervision for both public and private sector. - Parliament/Court/Constitutional Court/National Election Commission shall perform an independent function of protection. - KCC(on-line part)/FSC(credit information) shall perform the functions of policy-making/enforcement, in accordance with the respectively applicable law. - The head of a national administrative authority shall perform the duplicated function of policy-making and enforcement in its jurisdictional part of private sector. · The Personal Information Protection Commission under Prime Minister shall perform the deliberation function. · Commission for Mediation of Disputes on Personal Information (members are appointed by MoPAS Minister and the secretariat is within KISA). · Privacy Violation Complaints Center (part of KISA; a subsidiary for enforcement by MoPAS and KCC)

	<MoPAS Minister's functions of policy-making/enforcement/supervision> · Sets up a 3-year basin plan on personal information protection (the head of another national administrative agency shall set up a 1-year plan of implementation); · Creates and recommends the standard guidelines on personal information protection (the head of another national administrative agency shall create and recommend the guidelines for its jurisdictional area; · Promotes and supports self-regulation (education/publicity, support/assistance for protective groups, and support for certification marks and self-regulatory codes); · Recommends public agencies to register/publish/improve their personal information DB; · Administers the privacy impact statements of public agencies; · Gives his/her opinions on the laws and bylaws that have such provisions as may affect personal information protection; · Recommends improvements in the situation of personal information processing (the head of another national administrative agency shall make such recommendations for its jurisdictional area); · Receives/processes complaints on rights violations (the Privacy Violation Complaints Center) · Investigates into alleged violations (by requesting related documents/conducting site inspections) (the head of another national administrative agency shall make such investigations for its jurisdictional area); · Issues an enforcement order against violations (but a recommendation to the Parliament, etc.) (the head of another national administrative agency shall make such order for its jurisdictional area); · Files criminal charges against violations/recommends disciplines against the offenders (the head of another national administrative agency shall do so for its jurisdictional area); and · Imposes and collects monetary penalties (the head of another national administrative agency shall do so for its jurisdictional area)
Hye-hoon Lee bill	· The Personal Information Commission under the Prime Minister shall independently perform the functions of policy-making and supervision for both public and private sector. - The title of the Commission is intended to emphasize balanced promotion of the use and protection of personal information. - Main functions shall include counselling/rights remedies, education/publicity, technical development assistance and institutional improvements. - With the powers to request documents, investigate factual aspects, visit the premise for investigation purpose, issue a correction order, recommend correction and recommend for criminal charges/disciplines · The Commission for Mediation of Disputes on Personal Information shall be set up within the Personal Information Commission.
Jae-il Byun bill	· The Personal Information Protection Commission under the President shall independently perform the functions of policy-making/supervision for both public and private sector. - Shall promote a balance between the protection and the use of information. - With the powers to request documents, investigate factual aspects, visit the premise for investigation purpose, issue a correction order, recommend correction and recommend for criminal charges/disciplines · The Commission for Mediation of Disputes on Personal Information shall be set up within the Personal Information Commission.

3. Assessment of the enforcement structure in the Government bill

(1) Advocacy for the enforcement structure in the Government bill

Those who are supportive of the Government bill which provides for the comprehensive functions of policy making, enforcement and supervision argue that the structure may have some weaknesses in terms of independence and impartiality but can guarantee accountability, swiftness and strong execution. In other words, the advantages of the structure in the Government bill include: coherent policy execution, cooperation and support; efficient and swift remedies for rights violations; a strong power of law enforcement; and possible links between the personal information protection system and the data protection system, all of which can be expected of a national administrative authority.[22)]

In addition, the advocates say that "a multi-member commission may be reasonable for regulation and coordination which needs a relatively long time and a prudent process, but not good at setting up or operating promotional policies including a fundamental plan for personal information protection or making responsive decisions to address any difficulties, and this structure, in organizational terms, cannot manage a large number of government employees nor can it be flexible in personnel management in practice".[23)]

To sum up, the advocates argue that the Government bill is desirable, considering that the activities for personal information protection require a strong power of execution for prevention of leakage and abuse/misuse of personal data and for an immediate response to any violation and, especially in the initial years of law application, institutional systems to

---

22) Statement by Professor Heung-youl Youm at the public hearing on "Personal Information Protection Bill" of April 23, 2009 organized by the Parliamentary Committee on Public Administration and Security (pp. 3-4 of the public hearing material)

23) Statement by Counsel Sang-jik Lee at the public hearing on "Personal Information Protection Bill" of April 23, 2009 organized by the Parliamentary Committee on Public Administration and Security (pp. 24-25 of the public hearing material)

enforce security safeguards and increase the public awareness towards personal information protection, based on the strong executive power.

(2) Critical analysis of the Government bill

However, the Government bill seems to have several critical flaws:

First, it is not reasonable to require a single administrative authority to proceed with conflicting values at the same time. The Ministry of Public Administration and Security, which is in charge of the Electronic Government initiative, must be more inclined to the value of personal information use, in pursuit of the efficient establishment and operation of the e-Government.

In particular, the ideology of the e-Government initiative is disproportionately focused on the value of administrative efficiency and, therefore, the common use of personal information, which is one of the key words of the "E-Government Act". In step with the initiative, the Government has set up the "Committee to Promote Administrative Information Sharing" and the "Administrative Information Sharing Center", with a view to promote information sharing at intergovernmental level.[24] According to the basic directions for the structure of administrative information sharing and the role and functions of the Administrative Information Sharing Center, which are defined by the Committee to Promote Sharing of Administrative Information, the fundamental premise is to integrate and combine the personal information DBs and the business information DBs held by all administrative agencies. However, it is very alarming, especially in this free and democratic society, that the Government leaves open the possibility of integrating personal information DBs and business information DBs. The Government, in displaying "the common use of personal information"

24) For details on the developments about the common use of administrative information, see "2007 White Paper on the Common Use of Administrative Information" (pp. 24-140) published in December 2007 by the Committee to Promote Administrative Information Sharing.

as a key word and a precondition of the e-Government, is just emphasizing the functional efficiency of the Government while ignoring the values of administrative democracy and transparency.

Under these circumstances, it would be extremely difficult, although not impossible, for MoPAS to formulate and implement the policies on personal information protection which can coordinate the conflicting values. Moreover, the Ministry is a data processing agency with a vast amount of personal information, including resident registration DBs and land information DBs, and also shares personal information with other agencies. This means that the Ministry itself is subject to the supervision for its use of personal information. This is clearly contradictory to the natural justice 'Nobody can be a judge in his own case'.

Second, MoPAS can hardly guarantee independence and neutrality as it is a national administrative authority. The Minister is a political appointee, which means he/she has no fixed term of office and his/her term is highly affected by political conditions. The Ministers in Korea are particularly short-lived, and these short terms make it hard to proceed with coherent policies.

Third, MoPAS is not specifically designed for personal information protection and, therefore, is not specialized in that field. According to the "Government Organization Act", MoPAS is a national administrative authority which is to perform various responsibilities concerning: personnel management, service and pension of public servants; rewards and punishment for public servants; government reforms; the electronic government; the local autonomy system; administrative assistance for, finance and taxation of local governments; election; national referendum; safety management policies; emergency measures, civil defense and disaster control. This extensive scope of activities clearly shows that MoPAS is not a specialized agency for personal information protection. Even the public officials in charge of the work related to personal information protection cannot afford to obtain professional

expertise and experiences for this field, as they are subject to job rotation. As is said above, the work involved in personal information protection requires the professional expertise and knowledge on how to strike a delicate balance between the use and the protection of personal information. It would be too much to expect the non-professional Minister and MoPAS officials to perform the professional work of personal information protection work.

Fourth, the Government bill provides for separate roles of MoPAS, the Personal information Protection Commission, the Commission for Mediation of Disputes on Personal Information and the Privacy Violation Complaints Center, which makes it difficult to implement protective policies and carry out a supervising responsibility in an effective way. Furthermore, as for the private sector, the Minister of MoPAS and other national Ministers are supposed to exercise a duplicated power of execution. And as for the sectors of on-line services and credit information, KCC and FSC, without the current problems being resolved, are intended to play a protective role. After all, the Government bill does not envision a comprehensive and streamlined national system which guarantees coherence and coordination in policy making, execution and supervision.

Fifth, there is a concern about a broader gap of regulation between the public and the private sector. Even now, the supervision over the public sector is considerably weak whereas there exists an enforcement system marked with stringent *ex post facto* punishment for the private sector. The Government bill seems to aggravate this imbalance. It provides for exceptionally prohibitive criteria for protection in the private sector, raising concerns that the use of personal information might be unnecessarily discouraged in the private sector and, as a consequence, the private sector might lose economic vitality. It is the right time to contemplate why many advance nations place a higher emphasis on proactive supervision than on *ex post facto* punishment.

VI. Questions

I would like to ask some questions of Mr. Graham Greenleaf and Ms. Marie Georges with regard to the DPAs in Australia and European nations:

1. What are the reasons why Australia and some European nations have set up a separate supervisory body to protect personal information, instead of empowering the existing national human rights institution to perform the function? I understand that the Australian DPA was initially part of the national human rights institution and separated from the institution later in July 1, 2000. What are the background and the reasons of such separation?

2. In working for establishment of e-Government, have Australia and European nations adopted "the principle of common use of personal information"? Are there any attempts to combine and integrate personal information DBs held by public agencies?

3. In Australia and European nations, does the DPA issue a direct order of correction against law violations or impose monetary sanctions (including fines)?

4. How do the DPAs in those countries harmonize the two conflicting values involved in the "use" and the "protection" of personal information?

2
토 론

개인정보감독기구의 설립을 둘러싼 쟁점과 방향설정

이인호 (중앙대학교 법학전문대학원 교수)

목 차

I. 서 언

한국에서는 지난 2003년 이래 복잡한 개인정보보호체계를 체계적으로 정비하려는 노력이 정부와 시민단체, 그리고 학계에서 꾸준히 그리고 다각도로 이루어져 왔다. 다양한 개인정보보호법들이 공공부문과 민간부문으로 이원화되어 있고 여러 개별입법들이 존재하고 있어 개인정보처리기관이나 정보주체인 일반 국민의 입장에서 관련 법규에 대한 이해도가 낮아 법적 규율의 실효성이 떨어지고 있다. 또 민간부문에서는 일반법이 없어 일부 보호의 공백이 생기는 영역이 있는 등 문제점이 제기되었다. 그리하여 이를 개선하

려는 노력의 일환으로 공공과 민간의 모든 개인정보처리를 규율하는 통합 일반법을 제정하려는 움직임이 일어났다. 이러한 움직임은 2009년 9월 현재 3건의 「개인정보보호법안」으로 가시화되었다. 이혜훈 의원안, 변재일 의원안, 그리고 정부안이 국회에 제출되어 행정안전위원회에서 심의 중에 있다.

통합 일반법으로서의 개인정보보호법의 제정을 둘러싸고 여러 쟁점에서 첨예한 의견대립이 있다. 가장 기본적인 쟁점은 세 가지로 압축될 수 있는데, 첫째, 여러 영역에서 산발적으로 존재하는 여러 개별입법들을 체계적으로 어떻게 조정할 것인가 하는 입법체계에 관한 문제, 둘째, 이용과 보호의 가치를 합리적이고 균형 있게 조화시키는 개인정보 처리(=수집·이용·제공)의 입법기준이 무엇인가 하는 실체적인 문제(여기에는 개인정보처리의 허용기준, 절차적 요건, 정보주체의 참여권 등이 포함된다), 셋째, 그러한 법적 기준을 어떻게 집행할 것인가 하는 집행체계에 관한 문제, 특히 개인정보감독기구의 조직구성과 권한 및 기능을 어떻게 설정할 것인가 하는 문제를 들 수 있다.

이번에 국가인권위원회가 주최하는 「개인정보보호감독기구의 위상과 역할에 관한 국제심포지엄」은 위 쟁점들 중 마지막의 집행체계에 관한 문제를 집중적으로 다룬다. 이 심포지엄에서 발표를 맡아 주신 두 분의 세계적인 권위자(호주의 Graham Greenleaf 교수와 프랑스의 Marie GEORGES 자문관)의 풍부한 지식과 경험을 공유할 수 있게 된 것을 큰 기쁨으로 생각하며, 또 이 분들의 지식과 경험이 우리의 현안을 푸는 중요한 실마리가 될 것을 기대한다.

국회에서 심의 중인 3건의 「개인정보보호법안」은 공공부문과 민간부문 양 부문에 모두 적용되는 통합 일반법으로서, 검색이 가능한 데이터베이스(수기파일 포함)의 형태로 개인정보를 처리하는 모든 기관("개인정보처리기관")에게 공정한 처리(수집·이용·제3자 제공 등)의 법적 기준을 제시하고 그 기준의 준수를 집행 또는 감독할 기구를 마련함으로써, 한편에서는 개인정보의 적정한 이용을 허용하면서 동시에 다른 한편에서는 안전장치를 마련하여 프라이버시 등 정보주체의 권리나 이익이 함부로 침해되지 않도록 보호하고자 하는 것이다.

사실 「개인정보보호법」은 "사생활비밀보호법"이 아니다.[1] 때문에 「개인정보보호법」

1) 이인호, "제2세대 프라이버시보호법으로서의 개인정보보호법에 대한 이해", 사법 제8호 (사법발전재단, 2009. 6), 36-85면 참조.

은 개인정보의 “보호”만을 입법목적으로 하는 것이 아니라, 오히려 개인정보의 “안전한 이용”을 도모하고자 하는 데 그 근본취지가 있다. 개인정보의 무분별한 이용에 따르는 위험성(정보주체의 사생활침해, ID 도용에 의한 실제적 피해 등)을 예방하기 위한 안전장치를 둠으로써 사회에서 필요로 하는 개인정보의 이용을 원활하게 하고자 하는 데에 진정한 입법취지가 있다. 복잡한 현대사회가 정상적으로 기능하기 위해서는 개인정보의 이용과 유통이 필수적이다. 그러나 안전장치가 없는 무분별한 개인정보의 활용은 일반인들의 불안감만을 증폭시켜 오히려 사회적으로 필요한 개인정보의 유통마저도 차단시킬 염려가 있다. 따라서 사회적으로 필요한 개인정보의 이용과 유통이 적정하게 이루어지기 위해서는 무엇보다 안전장치의 확보가 전제되어야 한다.

그런데 이러한 안전장치 중의 하나가 바로 “독립된 개인정보감독기구”의 존재와 활동이다. 개인정보감독기구의 독립성이 강조되는 이유는 감독을 받는 개인정보처리기관이 바로 정부기관들이기 때문이다. 최근에는 기업과 같은 민간기관도 기업의 운영과 경제활동을 위해 방대한 개인정보데이터베이스를 구축하여 이용하고 있지만, 전통적으로 정부기관들은 소관업무의 수행을 위하여 국민 개개인의 개인정보를 데이터베이스화하여 처리하고 있다.[2] 따라서 개인정보를 처리하는 정부기관들이야말로 개인정보보호법의 규율을 받는, 그리하여 개인정보감독기구로부터 감독을 받는 전형적인 기관들이다. 그리하여 감독을 하는 자와 감독을 받는 자가 기능적으로 분리되어야함은 물론이고, 감독기구가 피감독기관으로부터 독립하여 독자적으로 감독업무를 수행할 수 있어야 한다.

여기서 중요한 요소는 감독기구의 “기능상의 독립성”이다. 개인정보감독기구의 독립성은 조직체계상으로 완전한 분리 독립을 의미하는 것이라기보다 기능상의 분리 독립을 의미한다. 따라서 개인정보감독기구를 조직체계상으로 대통령이나 국무총리 소속 하에 둔다고 해서 그 자체만으로 독립성이 없다고 단정할 수는 없다.

그리하여 지난 17대 국회에 발의되어 자동 폐기되었던 3건의「개인정보보호법안」들은 개인정보감독기구의 독립성을 확보하기 위하여 개인정보보호위원회를 국무총리 소속하에 두거나, 국가인권위원회 성격의 독립성을 제안하고 있었다. 그런데 올해 6월 27일 행

2) 2006년 전체 공공기관이 보유하고 있는 개인정보데이터베이스(“개인정보화일”)는 총 1144개이다. 이 중 중앙행정기관이 277개, 지방자치단체 397개, 교육기관 67개, 정부투자기관 등이 403개를 보유하고 있다. 행정자치부, 공공기관의 개인정보화일목록집, 2006 참조.

정안전부가 개최한 제1차 공청회에서 제시된 법안설명에서는 행정안전부장관이 개인정보보호법의 집행 및 감독책임을 지는 주무부처이고 그 소속 하에 분쟁조정기능만을 주된 업무로 하는 개인정보분쟁조정위원회를 두도록 하고 있었다.[3] 이에 대해 진보넷 등의 시민단체와 일부 논자들은 법안이 개인정보감독기구의 독립성을 포기한 것이라고 비판하였다. 비판의견을 수렴한 행정안전부는 8월 12일 「개인정보보호법 제정법률안」을 정식으로 입법예고하고 8월 28일 제2차 공청회를 열고 정부안으로 국회에 제출되어 심의 중에 있다.

정부안에 의하면, 행정안전부장관이 집행 및 감독책임을 지는 주무부처이고 개인정보분쟁조정위원회가 분쟁조정기능을 수행하되, 몇 가지 사항에 대해 심의기능을 하는 개인정보보호위원회를 신설하여 국무총리 소속 하에 두는 것으로 하고 있다. 이 법안의 개인정보보호위원회를 개인정보감독기구라고 볼 수 있는지, 그리고 법안상의 집행 및 감독체계를 독립된 감독체계라고 볼 수 있는지가 문제되고 있다.

II. 전문적이고 독립된 개인정보감독기구의 존재이유

(ⅰ) 개인정보의 처리와 관련한 집행의 문제는 당해 정보주체가 인식하지도 못한 상태에서 개인정보가 정부나 기업에 의해 광범위하게 수집 · 축적 · 처리 · 제3자 제공 내지 공유된다는 사실에 있음. 자신의 개인정보에 대한 침해사실을 인식조차 하지 못하는 정보주체가 권리구제절차를 밟을 수 있는 가능성이 희박함

(ⅱ) 설령 개인정보처리의 원칙 중 수집제한의 원칙과 시스템공개의 원칙이 잘 지켜져 개인정보의 수집과 처리에 대한 정보주체의 인식이 있다 하더라도, 처리기관 내부에서 이루어지는 위법적인 상황을 외부자인 정보주체가 충분히 파악할 수 없을 뿐만 아니라 조사할 수도 없음. 기술적으로 복잡한 처리과정이나 은밀하게 이루어지는 목적 외 이용 및 제3자 제공에 관한 상황을 외부의 비전문가인 정보주체가 제대로 알 수 없기 때문임

3) 행정안전부, 「개인정보보호법」 제정을 위한 공청회 자료집, 2008. 6. 27 참조.

(iii) 더 나아가, 설령 그것을 정보주체가 충분히 파악했다고 하더라도, 자신의 노력과 주도 하에 법원을 통한 그 복잡하고 장기적인 소송절차를 밟아서 권리구제를 받는다는 것은 결코 손쉬운 일이 아님. 또한 법원을 통한 권리구제는 언제나 사후적인 것임. 개인정보보호에 있어서는 예방적인 권리구제가 더욱 절실히 요청됨

(iv) 통상 개인정보DB에 의한 개인정보처리는 특정 개인이 아니라 수많은 개인들을 대상으로 하는 것이기 때문에 위법적인 개인정보처리의 영향은 그들 모두에게 똑 같이 미칠 수 있음. 즉 위법한 개인정보처리에 따르는 피해는 대규모적이고 집단적인 성격을 지님

(v) 공공부문에 있어서 개인정보감독기구는 그 기능이 독립적으로 이루어져야 할 필요가 있음. 개인정보보호의 가치는 개인정보처리를 통해 얻어지는 효율성의 가치와 상충될 수밖에 없음

요컨대, 정부나 기업에 의한 위법한 개인정보처리로부터 정보주체의 개인정보자기결정권을 실질적으로 보장하기 위해서는 예방적이고 사전적인 차원에서 개인정보처리를 감시·감독하며, 또 피해가 발생한 경우 법원의 소송절차 외에 보다 효과적이고 효율적인 권리구제를 실질적으로 가능하게 해주는 독립된 개인정보감독기구의 존재가 필수적이다.

개인정보보호를 위한 독립된 감독기구가 필요하다는 인식은 개인정보보호 분야에서 세계적 권위를 자랑하는 뛰어난 분석가들에 의해서도 확인되고 있다. 캐나다의 Colin J. Bennett 교수(University of Victoria)와 영국의 Charles D. Raab 교수(University of Edinburgh)는 이렇게 분석하고 있다. "강력한 감독기구의 존재는 훌륭한 프라이버시 보호체계의 필수조건(sine qua non)으로 간주되어 오고 있다. 왜냐하면 법이란 스스로 집행되는 것이 아니고, 또 프라이버시 문화는 권위 있는 옹호자가 없이는 그 스스로 확립될 수 없기 때문이다."[4]

또한 일찍이 캐나다의 British Columbia주의 개인정보보호청장이었던 David Flaherty도

4) Colin J. Bennett & Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Ashgate, 2003), p. 107.

"개인정보감독기구는 프라이버시 보호를 위한 일종의 경보체계이다(an alarm system for the protection of privacy)."고 역설하였다.[5)]

요컨대, 이제 개인정보보호를 위한 독립된 감독기구의 설립은 더 이상 선택의 문제가 아니다. OECD 회원국으로서, 그리고 세계 12대 교역국인 우리나라는 국제규범에 충실할 필요가 있으며, 또한 정보기술의 강국으로서 21세기 인간존엄이 보장되는 고도정보사회로의 기반을 조성하기 위해서는 독립된 개인정보감독기구의 존재가 필수적이라고 하겠다.

세계 각국은 유럽연합 개인정보보호지침(95/46/EC)의 주도적인 영향 하에서 공공부문과 민간부문을 통합하여 감독하는 단일의 개인정보감독기구를 설립하는 추세를 보이고 있다. 이 추세는 비단 유럽연합이나 유럽평의회 회원국에 한정되는 것이 아니고 비회원국들도 새로운 개인정보보호법을 제정하면서 독립된 통합감독기구를 설립하고 있음을 볼 수 있다. 그 경향을 정리하면 아래 표와 같다.[6)]

<표 1> 유럽평의회 회원국의 감독기구 현황

국가명	개인정보감독기구	홈페이지	국가명	개인정보감독기구	홈페이지
오스트리아	Büro der Daten-schutzkommission	www.dsk.gv.at	룩셈부르크	Commission nationale de la protection des données	www.cnpd.lu
벨기에	Commission de la Protection de la vie privée	www.privacy.fgov.be	네덜란드	College Bescherming Persoonsgegevens	www.dutchdpa.nl
불가리아	Personal Data Protection Commission	www.cpdp.bg	노르웨이	Datatylsinet	www.datatilsynet.no
크로아티아	Personal Data Protection Agency	www.azop.hr	폴란드	Bureau of Inspector General for Personal Data Protection	www.giodo.gov.pl
키프로스	Office of Personal Data Protection Commissioner	www.dataprotection.gov.cy	포르투갈	Commissão Nacional de Protecção de Dados	www.cnpd.pt

5) David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (1989), p. 383.

6) 이 표의 내용은 유럽평의회(Council of Europe) 홈페이지에 게시된 내용을 정리한 것임. <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Supervisory_authorities/>

국가명	개인정보감독기구	홈페이지	국가명	개인정보감독기구	홈페이지
체코공화국	Office for Personal Data Protection	www.uoou.cz	루마니아	National Supervisory Authority for Personal Data Processing	www.dataprotection.ro
덴마크	Datatilsynet	www.datatilsynet.dk	슬로바키아	Commissioner For Personal Data Protection	www.dataprotection.gov.sk
핀란드	Office of Data Protection Ombudsman	www.tietosuoja.fi	슬로베니아	Information Commissioner	www.ip-rs.si
프랑스	Commission Nationale de l'Informatique et des Libertés	www.cnil.fr	스페인	Agencia Española de Protección de Datos	www.agpd.es
독일	Bundesbeauftragte für den Datenschutz	www.datenschutz.de	스웨덴	Datainspektionen	www.datainspektionen.se
그리스	Data Protection Commission	www.dpa.gr	스위스	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter	www.edoeb.admin.ch
헝가리	Data Protection Commissioner	www.obh.hu	영국	Office of the Information Commissioner	www.ico.gov.uk
아이슬란드	Persónuvernd (Data Processing Authority)	www.personuvernd.is	이탈리아	Garante per la protezione dei dati personali	www.garanteprivacy.it
아일랜드	Data Protection Commissioner	www.dataprivacy.ie	에스토니아	Inspection of Data Protection	www.dp.gov.ee

<표 2> 유럽평의회 비회원국의 감독기구 현황

국가명	개인정보감독기구	홈페이지	국가명	개인정보감독기구	홈페이지
캐나다	Privacy Commissioner	www.privcom.gc.ca	호주	Privacy Commissioner	www.privacy.gov.au
홍콩	Office of the Privacy Commissioner for Persona Data	www.pco.org.hk	모나코	Commission de contrôle des informations nominatives	www.ccin.mc
뉴질랜드	Privacy Commissioner	www.privacy.org.nz	태국	Official Information Commission's Office	www.oic.thaigov.go.th

III. 개인정보감독기구의 기능과 권한

세계 각국의 개인정보감독기구는 7가지의 서로 연관된 역할과 기능을 수행하고 있는 것으로 분석된다. ① 옴부즈맨(ombudsmen)으로서, ② 감사관(auditor)으로서, ③ 자문역(consultant)으로서, ④ 교육자(educator)로서, ⑤ 교섭자(negotiator)로서, ⑥ 정책조언자(policy adviser)로서, 그리고 ⑦ 집행자(enforcer)로서의 역할과 기능이 그것이다.

물론 모든 감독기구가 이 모든 역할을 동일한 비중을 가지고 수행하는 것은 아니다. 또한 이들 기능이 개인정보감독기구에 의해서만 배타적으로 수행되는 것도 아니다. 일부 국가에서는 다른 정부부처도 개인정보보호에 있어서 중요한 책임을 떠맡기도 한다. 이하에서는 이들 기능에 대하여 구체적으로 살핀다.[7]

1. 옴부즈맨(ombudsmen)으로서의 개인정보감독기구

우선 모든 개인정보감독기구들은 정보주체로부터의 불만이나 민원(complaints)을 접수받고, 사실관계를 조사하며, 그리고 그 민원사항을 해결하는 기능을 수행한다. 이러한 "민원의 접수·조사·해결"이라고 하는 옴부즈맨의 전통적인 기능은 모든 개인정보보호체계의 효율적인 감독기능에 있어서 가장 핵심적인 것이다. 물론 그것은 시간을 소요하고 상당한 자원을 필요로 하는 일이다.

이러한 민원처리시스템을 구축함에 있어서는 그 기능이 원활히 수행되기 위해서 어떤 권한들이 감독기구에 주어져야 할 것인지에 대해서 면밀한 검토가 필요하다. 국가마다 다양성이 있긴 하지만, 대체로 이들 권한으로는 i) 개인정보처리기관의 구내에 출입하는 권한, ii) 개인정보처리과정에서 산출된 관련 기록을 요구할 수 있는 권한, 그리고 iii) 개인정보처리에 책임이 있는 자를 소환할 수 있는 권한을 들 수 있다. 이와 관련해서 한 가지 어려운 문제는, 정보주체에 의한 민원신청이 없더라도 감독기구가 독자적으로 법위반사실을 조사할 수 있는 권한을 행사할 수 있을 것인가 하는 문제이다. 일부 국가에서는 감독기구의 직권에 의한 조사권한을 부여하고 있다.

한편, 민원해결의 방식은 매우 다양한 형태를 가질 수 있는데, 예컨대 영국에서와 같

7) 이들 기능에 대한 설명은 Colin J. Bennett & Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Ashgate, 2003), pp. 109-114에서 크게 참조함.

이 구속력 있는 집행명령(binding enforcement order)의 형태에서부터 캐나다, 뉴질랜드, 호주와 같이 구속력이 약한 권고(less mandatory recommendations)에 이르기까지 다양하다. 화해(conciliation)와 조정(mediation)에 의존하는 감독기구들은 개인정보처리기관이 일반인에게 나쁜 이미지를 심어주지 않기 위해서 민원제기에 대해 적극적으로 화해를 하려고 하는 경향에 의존하게 되는데, 감독기구로서는 그러한 경향을 적극 활용하여야 한다.

2. 감사관(auditor)으로서의 개인정보감독기구

민원의 조사와 해결은 그 본질이 수동적이고 소극적인 과정이다. 그러나 개인정보감독기구는 여러 정보에 근거해서 특정 개인정보처리기관의 처리행태에 대해 의심을 가질 수 있으며, 따라서 그 기관이나 특정 기술에 대하여 보다 일반적인 감사를 실시할 수 있다. 감사(audits)는 보다 체계적일 뿐만 아니라 구체적인 민원제기에 따른 조사에 비하면 덜 대립적이다.

독일의 연방정보보호청은 그 설립 초기부터 개인정보처리시스템에 대한 감사를 실시해 오고 있다.[8] 독일의 감독기구들은 한 개인정보처리기관 내에서 이루어지는 개인정보처리의 모든 측면에 대한 조사기법을 발전시켜 왔다.[9]

감사는 그것을 얼마나 자주 행하느냐 그리고 얼마나 엄격하느냐에 따라 다양한 유형을 지닌다. 캐나다와 같은 국가에서는, 감사프로그램(an audit programme)은 비록 연방프라이버시법(Privacy Act)에서 그것을 명문화하고 있지는 않았지만 처음부터 연방프라이버시보호청의 상시적인 업무의 하나가 되어 왔다. 그 밖에 캐나다의 주 차원에서는 보다 비공식적인 현장방문(site visit)이 행하여질 수 있다. 예컨대, 캐나다의 British Columbia주의 개인정보보호청장이었던 David Flaherty는 보호청장 당시 당해 주의 대규모 공공기관에 대하여 비공식적이고 부담을 주지 않는 형태의 현장방문을 촉구하기도 하였다고 한다.[10]

---

8) David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (1989), p. 77.

9) Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press, 1992), p. 182.

10) David H. Flaherty, "How to Do a Privacy and Freedom of Information Act Site Visit"

한편, 일부 국가의 보호법은 명시적으로 감독기구에게 감사기능을 부여하고 있다. 예컨대, 캐나다 연방 차원의 민간부문 개인정보보호법인「개인정보보호 및 전자문서법」(Personal Information Protection and Electronic Documents Act)은 감사기능이 주의 개인정보보호청이나 회계법인 또는 표준인증기구에게 위임될 수 있음을 예정하고 있다. 또한 네덜란드의 개인정보보호청장은 일정한 경우에는 공인된 감사기관에 의해서 감사가 실시되도록 요구하고 있다.

3. 자문역(consultant)으로서 개인정보감독기구

각 국의 모든 개인정보감독기구들은 각 개별 개인정보처리기관에게 어떻게 하면 개인정보보호법을 준수할 수 있는지에 관하여 언제나 조언과 자문을 행한다. 개인정보보호법의 이행은 법적 권한의 존부를 떠나서 개인정보감독기구가 얼마나 자문기능을 충실히 수행하느냐에 달려 있다고 해도 과언이 아니다. 사후에 강제력을 발동하기보다는 사전에 개인정보보호시스템을 갖추도록 장려하고 조언하는 것이 무엇보다 중요하다. 자문과 조언은 규제자와 피규제자라는 대립적 관계보다 훨씬 더 나은 것으로 간주되고 있는데, 대립적인 관계는 많은 비용을 요하고 비효율적일 수 있기 때문이다.

특히 프라이버시 침해적인 새로운 기술이나 시스템을 도입하는 경우에 개인정보감독기구의 자문역할과 기능은 매우 중요한 의미를 지닌다. 통상 개인정보처리기관들은 도입을 계획하고 있는 시스템이 개인정보보호법을 준수하게 되는지 여부를 미리 알고자 한다. 이러한 자문기능은 흔히 공식적인 절차 밖에서 이루어지는 경향이 있는데, 이 때 감독기구는 나중에 당해 처리기관에 대한 민원이 제기되지 않도록 그 자문과 조언을 그 독립성이 훼손되지 않는 선에서 신중하고 공정하게 할 수 있도록 조심해야 할 것이다.

4. 교육자(educator)로서의 개인정보감독기구

개별적인 자문기능 외에, 개인정보감독기구는 보다 광범위한 교육 및 연구기능을 수행한다. 보다 큰 차원에서 감시의 문제와 프라이버시 문제를 분석·연구하고 또 개인정보처리기관과 정보주체들을 계속해서 교육시키며 정부와 사회 전반에 걸쳐 프라이버시 보

<http://www.oipcbc.org/> 참조.

호 문화를 촉진시키는 것은 매우 중요한 기능이다. 세계의 모든 감독기구는 이러한 기능을 부여받고 있으며, 다만 그 활동범위와 강도에 있어서 다양한 차이를 보이고 있다.

비록 한정된 자원이긴 하지만, 개인정보감독기구는 개인정보보호의 이념과 보호원칙들을 이해시키고 프라이버시보호문화를 신장하는 데 주력할 필요가 있다. 세계적으로도 각국의 감독기구들은 이러한 기능과 관련해서 흥미 있는 사례들을 보여주고 있다.

예컨대, 캐나다의 연방프라이버시보호청(Office of the Privacy Commissioner of Canada)은 민간부문의 일반법인 「개인정보보호 및 전자문서법」의 내용을 일반인에게 정확히 그리고 널리 알리기 위해 "기업과 단체를 위한 지침"(Guide for Businesses and Organizations)을 공표하고 있다.[11] 이 지침은 법률의 이행을 확보하기 위하여 법률의 규율범위, 공정정보처리의 원칙들, 권리구제절차 등을 알기 쉬운 언어로 풀어서 상세하게 설명하고 있다. 그 밖에도 캐나다의 연방프라이버시보호청은 기업들이 어떻게 하면 이 법률을 준수할 수 있는지를 돕기 위하여 여러 가지 정보들을 제공하고 있다.[12] 한편, 캐나다 Ontario주의 감독기구인 「정보 및 프라이버시보호청」은 개인정보보호원칙의 준수 여부에 대한 자가진단과 자체평가를 돕기 위하여 "프라이버시 진단 툴"(Privacy Diagnostic Tool)을 주요 회계법인들과 공동으로 개발하여 공표해 놓고 있다.[13]

그 밖에도 각국의 감독기구들은 이처럼 법준수를 위한 자가진단프로그램을 개발하는 데 상당한 노력을 하고 있다. 예컨대, 홍콩의 프라이버시보호청(PCO: Office of Privacy Commissioner for Personal Data)은 2000년에 공공부문과 민간부문의 개인정보처리기관들이 개인정보보호법(Personal Data [Privacy] Ordinance)의 준수 여부에 대한 자체평가를 돕기 위하여 "Privacy.SAFE: Guidance Notes for Self-Assessment"를 개발하여 공표하였다.

이처럼 각국의 감독기구들은 특별한 영역이나 기술 분야에 있어서의 프라이버시 쟁점들을 조사하고 그 해결방안을 연구하며 때때로 여론조사를 수행하기도 한다. 그 연구결과물인 각종의 보고서들은 새로운 기술에 내재된 프라이버시위험을 정부나 기업 그리고 일반인에게 경고하는 매우 유용한 수단으로 활용되고 있다.

---

11) 이 지침의 내용은 <http://www.privcom.gc.ca/information/guide_e.asp> 참조.
12) 이들 정보자원들은 <http://www.privcom.gc.ca/ekit/ekit_e.asp>에서 확인할 수 있다.
13) "프라이버시 진단 툴"의 내용은 <http://www.privcom.gc.ca/ekit/ct_01_e.asp> 참조

5. 정책조언자(policy adviser)로서의 개인정보감독기구

각국의 개인정보보호법은 대부분 개인정보감독기구에게 새로운 입법안이 프라이버시 보호에 어떤 의미를 지니는지, 그리고 새로 도입되는 자동개인기록시스템이 어떤 영향을 미칠 것인지에 대하여 논평이나 조언을 하는 책무를 부여하고 있다. 예컨대, 캐나다의 공공부문 보호법인 「프라이버시법」(Privacy Act)은 연방프라이버시보호청에게 그 관할 범위 내에서 특정 쟁점에 관하여 의회에게 특별보고를 할 수 있는 권한을 부여하고 있다.[14]

많은 나라에서 그러하지만, 예컨대 캐나다의 경우 연방프라이버시보호청은 인구조사 과정(census process)에서 항상 연방정부와 충돌과 갈등을 빚고 있다.[15] 한편, 영국의 경우 정보보호청장은 정부의 공공서비스 확대와 사기방지를 위한 광범위한 정보공유(data-sharing)를 계획하는 정부안에 대하여 그것이 가지는 프라이버시 영향에 관하여 정책적 조언을 한 바 있다.[16] 그리고 일부 국가에서는 새로운 기술이 도입될 때마다 "프라이버시영향평가서"(privacy impact statement)를 작성하도록 요구된다.[17]

또한 각국의 감독기구들은 의회의 청문절차에서 흔히 관련 쟁점에 관해 증언을 하기도 하고, 정부의 정책에 대응해서 반대 입장을 공식적으로 표명하기도 한다. 후자의 잘 알려진 사례로서는 1995년에 영국의 내무부(Home Office)가 추진하려고 했던 신분카드제에 대해 당시의 감독기구였던 정보등록청(UK Registrar: 지금의 Information Commissioner의 전신)이 깊은 우려를 표명한 사례를 들 수 있다. 당시 정보등록청은 내무부의 사실조사와는 별도로 신분카드제에 대한 국민의 태도를 자체 조사하여 그 결과를 공표하였다.

6. 자율규제의 조정자(negotiator)로서의 개인정보감독기구

일부 국가의 개인정보감독기구는 민간기관의 자율규제규범인 실무규약(privacy code

14) Privacy Act, Sec. 39(1).

15) Canada, Office of the Privacy Commissioner (OPC), Annual Report 1999-2000 (Minister of Public Works and Government Services Canada, Ottawa, 2000), pp. 49-52 참조.

16) United Kingdom, Performance and Innovation Unit, Cabinet Office, Privacy and Data-Sharing: The Way Forward for Public Services (Cabinet Office, 2002) 참조.
<http://www.number-10.gov.uk/su/privacy/downloads/piu-data.pdf>

17) 미국과 캐나다의 프라이버시영향평가제도에 관해서는 구병문, "프라이버시 영향평가 제도의 국내법적 도입방안 - 공공부문을 중심으로 -", 「제3차 개인정보보호 정책 포럼」(정부혁신지방분권위원회, 2004. 6. 16), 38-46면; 이규정 · 구병문, 『공공부문 프라이버시 영향평가제도』(한국전산원, 2003) 참조.

of practice)에 대하여 협상하는 책무를 명시적으로 부여받고 있다.

자율규제규범으로서의 실무규약은 비록 국가법인 개인정보보호법이 존재하더라도 그 자체 뚜렷한 장점을 가지고 있다. 이 실무규약을 협상하는 과정에서 여러 상이한 부문과 영역에서 독특하게 안고 있는 프라이버시 문제에 대하여 상호 이해를 증진시킬 수 있다. 실무규약은 매우 유연한 규범이며 경제상황과 기술발전의 변화에 쉽게 적응해 나갈 수 있다. 실무규약은 또한 개인정보처리기관들이 자신들의 개인정보보호정책(privacy policy)을 공표하게 함으로써 부당한 개인정보처리행태에 관한 의심을 제거할 수 있게 하여 준다. 요컨대, 실무규약은 감독기구와 개인정보처리기관 상호간의 이해를 증진시키는 데 크게 기여할 수 있다.

그러나 자율규제규범인 실무규약과 국가법인 개인정보보호법의 관계와 관련해서 아주 어려운 문제가 있다. 실무규약을 활용하거나 장려해 온 국가들의 사례를 분석해 보면 거기에는 미묘한 차이를 지닌 3가지 모델을 발견할 수 있다.

첫째, 가장 엄격한 모델로서, 뉴질랜드의 「프라이버시법」(Privacy Act)이 채택하고 있는 방식이다.[18] 뉴질랜드 방식의 핵심 포인트는 「프라이버시법」에 따라 협의하여 결정된 실무규약은 법적 구속력(force of law)을 가진다는 점이다. 따라서 승인된 실무규약을 위반하는 것은 프라이버시법에서 명시한 개인정보보호원칙을 위반하는 것과 동일하고, 그 결과 법이 정한 민원처리절차 및 집행절차가 작동하게 된다.

두 번째 모델은 다소 유연한 방식으로서 네덜란드의 방식을 들 수 있다. 네덜란드 방식은 많은 점에서 뉴질랜드와 비슷하고 또 실무규약에 대한 신중한 협상과정을 담고 있긴 하지만, 종국적으로 그 실무규약은 법원에 대하여 정식의 구속력을 가지지 않는다. 물론 만일 특정의 개인정보처리기관이 그 실무규약이 요구하는 사항들을 준수하였음을 입증할 수 있다면, 그것은 상당한 설득력을 가질 수 있을 것이다. 그러나 역으로, 실무규약의 규정을 위반하였다는 원고의 입증이 있다면, 그것은 개인정보보호법에 따른 책임을 근거지우는 일응의 증거(prima facie evidence)가 된다. 그러므로 실무규약은 직접적인 것은 아니지만 간접적인 법적 효과를 갖는다.

세 번째 모델은 영국과 캐나다가 취하는 방식으로서, 개인정보보호법이 단순히 감독기구에게 실무규약의 제정을 촉구하는 권한을 주고 있는 모델이다. 이 모델에 있어서 실

18) New Zealand Privacy Act 1993, Secs. 46-53.

무규약은 간접적인 법적 효과마저도 갖지 않는다. 사실 이 세 번째 모델은 유럽연합의 개인정보보호지침(Directive 95/46/EC) 제27조가 예정하고 있는 바이다.

포괄적인 개인정보보호법을 가지고 있는 입법체계에 있어서 이 자율규제규범인 실무규약의 활용에는 중요한 딜레마가 놓여 있는 것으로 보인다. 만일 감독기구가 실무규약을 정식으로 승인하지 않는다면, 그 실무규약에는 개인정보보호법의 내용과 상충하는 내용이 담길 수 있고 그렇게 되면 법의 적용과 집행에 있어서 혼란이 야기될 수도 있다. 그러나 한편으로, 만일 뉴질랜드와 네덜란드와 같이 보다 정식의 승인절차가 있는 경우에는, 그것은 본래 자율규제의 유연성을 인정하고자 의도된 실무규약의 제정을 관료화하는 결과가 초래될 수 있다.

7. 집행자(enforcer)로서의 개인정보감독기구

개인정보감독기구의 기능과 권한 중에 개인정보보호원칙의 이행을 직접 명령할 수 있는 권한을 부여할 것인가 하는 점이 중요한 문제가 된다. 이 집행권한은 개인정보처리기관의 행위를 변경하도록 직접 명령하는 것으로서, 조사 및 권고기능과는 구별된다.

논자에 따라서는 집행자로서의 기능보다는 권고적 기능에 더 중점을 두어야 한다는 주장이 있다. 그리고 만일 개인정보처리기관이 개인정보보호에 충실하지 못한 행태를 보이는 경우 그 사실을 일반인에게 공표하는 것만으로도 매우 효과적인 제재가 될 수 있다고 주장한다.

그러나 한편으로, 다른 논자들은 설령 집행권한이 드물게 행사되더라도 그 권한의 존재 자체가 개인정보처리기관의 법 준수를 이끌어내는 효과적인 기능을 수행한다고 주장한다. 더구나 개인정보처리기관인 공공기관과 민간기관은 개인정보보호원칙을 적용함에 있어서 확실성과 일관성을 유지할 필요가 있다. 정식의 집행권한을 행사하는 절차는 시간이 흐름에 따라 법의 적용에 있어서 매우 높은 수준의 일관성과 투명성, 그리고 책임성을 보장해 줄 수 있을 것이다. 그리하여 시간이 흐름에 따라 법이 준수되는 비율을 높일 수 있을 것이다.

대부분 국가들의 개인정보보호법에서는 종국적인 권리구제는 법원에서 이루어지도록 하고 있고, 감독기구에 의한 민원해결절차에 대해서는 법원에서 재심사할 수 있도록 하고 있다. 한편, 일부 국가에서는 비교적 전문적이고 기술적인 분쟁을 다루기에는 법원이

반드시 가장 적합한 기관은 아니라는 판단 하에, 준사법적 기능(quasi-judicial function)을 수행하는 전문가집단으로 구성되는 소규모의 심판원(tribunal)을 설립하고 있다. 예컨대, 영국은 1998년의 개인정보보호법(Data Protection Act)에서 정보보호심판원(Data Protection Tribunal)을 설립하고, 정보보호청장(Information Commissioner)의 결정에 불복하고자 하는 개인이나 개인정보처리기관이 정보보호심판원에 불복신청을 할 수 있도록 하고 있다. 이 심판원은 필요하다면 전문가패널로 구성되기도 한다.

IV. 개인정보감독기구의 설립방향

일반적으로 개인정보감독기구는 집행권한을 가진 전통적인 행정기관은 아니다. 또한 반드시 국가의 정보정책에 관한 결정기관일 필요도 없다.[19]

개인정보감독기구의 주된 기능은 크게 **예방적 기능**, **사후적 민원해결기능**, **정책조언기능**의 세 가지로 분류할 수 있다. 첫째, 개인정보처리의 위험성을 사전적·예방적인 차원에서 막기 위하여 개인정보처리기관이 개인정보보호법의 실체적 규정, 즉 개인정보처리원칙을 구체화한 의무규정들을 준수하도록 사전에 유도하는 기능이다("예방적 기능"). 위에서 살핀 감사기능, 자문기능, 교육기능, 그리고 자율규제의 조정자로서의 기능은 이러한 예방적 기능의 일환이다.

둘째, 사후적인 민원해결기능이다. 즉 정보주체로부터의 불만이나 민원을 접수받고, 사실관계를 조사하며, 그리고 그 민원사항을 해결하는 기능을 수행한다. 이러한 "민원의 접수·조사·해결"이라고 하는 옴부즈맨의 전통적인 기능은 모든 개인정보보호체계의 효율적인 감독기능에 있어서 핵심적인 것이라고 하겠다. 물론 민원의 해결방식은 침해의 태양에 따라 다양할 수 있다. 화해를 유도하거나, 손해가 발생한 경우 조정절차를 진행하거나, 일정한 경우에는 민원인을 대신하여 법원에 소송을 제기하거나, 형사처벌에 해당하는 중대한 법위반인 경우에는 검찰에 고발하거나, 또는 행정적 제재권한을 가진 집행기관에게 행정적 제재(징계 또는 과태료부과 등)를 권유하는 등 다양하다.

---

19) 김일환 교수는 개인정보감독기구는 "직접적인 민주적 정당성의 결여 때문에 입법부나 행정부 대신에 감독기구가 정보정책에 관한 결정들을 내리는 것은 정당하지도 않고 적합하지도 않다."고 지적하고 있다. 김일환, 『개인정보보호법제의 정비방안에 관한 연구』(한국법제연구원, 1997), 198면.

셋째, 국가의 정보정책에 대한 조언자로서의 기능을 들 수 있다("정책조언기능"). 정책을 결정하고 입안하는 기능은 행정부와 입법부가 담당하는 몫이고, 개인정보감독기구는 그러한 정책결정에 조언하는 기능을 수행할 수 있고, 또 그러해야 한다.

향후 설립될 감독기구는 이상의 세 가지 기능을 마땅히 수행해야 하고, 그러한 기능의 수행에 필요한 권한을 가져야 하며, 그리고 그 기능과 권한을 원활하게 수행하기 위해서는 조직의 구성과 예산확보의 측면에서 충분한 독립성이 확보되어야 한다.

다만, 새로운 감독기구에게 집행권한을 줄 것인가 하는 문제는 우리의 현실상황과 연관하여 진지한 검토가 필요하다. 이 집행권한은 개인정보보호법의 이행을 위해 개인정보처리기관의 행위를 변경하도록 직접 명령하는 권한이다. 예컨대, 개인정보처리원칙을 구체화한 개인정보보호법의 규정들을 위반하여 개인정보를 처리한 경우 당해 개인정보의 처리를 중지시키거나, 또는 개인정보처리시스템의 작동을 중지시키는 명령을 내리는 것이다. 그리고 이 명령 위반에 대해 과태료 등의 제재권한을 발동할 수도 있을 것이다. 이러한 행정처분권, 즉 집행권한을 가지는 감독기구는 전통적인 행정기관의 성격도 아울러 가지게 된다. 예컨대, 현재의 공정거래위원회나 방송통신위원회와 같은 성격을 갖게 될 것이다.

그런데 감독기구는 민간부문뿐만 아니라 공공부문도 그 감독의 대상으로 하기 때문에 공공기관에 대하여 이렇게 강력한 집행권한을 행사하는 것이 그 실효성 측면에서 과연 타당한지는 다소 의문이다. 판단컨대, 공공기관의 위법행위를 시정하는 방법으로서 반드시 직접적인 명령에 의하는 것만이 유일한 것은 아니다. 간접적인 집행방법이 얼마든지 가능하고 또 유효할 수 있다. 예컨대, 위법사실의 공표, 국회나 상급감독기관에의 통지, 여론조성 등의 다양한 방법에 의하여도 공공기관의 법위반을 효과적으로 시정할 수 있다.

따라서 새로운 제도를 도입하는 현 시점에서는 처음부터 강력한 집행권한을 가진 감독기구를 마련하기보다는, 기존의 제도나 기관과의 마찰을 최소화할 수 있는 형태로 감독기구를 구성할 필요가 있다고 생각된다. 감독기구의 위 세 가지 기본기능, 즉 예방적 기능, 사후적 민원해결기능, 정책조언기능의 활성화에 집중해서 그것을 제도화하고, 또 설립 이후 감독기구의 역량을 최대한 발휘하여 효과적인 개인정보보호체계를 갖추어나가는 것이 현 시점과 현 상황에서 우선되어야 할 과제라고 하겠다.

한편, 독립된 감독기구가 존재한다고 해서 그것이 곧 바로 효과적인 개인정보보호체계의 확립으로 이어지는 것은 아니다. 공공과 민간의 그 수많은 개별 개인정보처리기관

에 대해 한정된 자원의 감독기구가 일일이 감독기능을 수행할 수도 없다. 때문에 공공기관과 민간의 각 개인정보처리기관의 내부에 독립적인 위상과 독자적인 기능을 가진 개인정보보호책임자(CPO: Chief of Privacy Official)를 반드시 두도록 해야 할 것이다. 이 개인정보보호책임자가 당해 기관 내부의 개인정보처리를 감독하고 개인정보보호법을 준수하도록 하는 1차적인 감독기능을 수행하는 것이 무엇보다 중요하고 필요하다. 이 기관 내부의 개인정보보호책임자는 당해 기관에 소속된 자이지만, 기능적으로는 개인정보감독기구의 현장감사관이 되는 것이다.

V. 정부안의 집행체계에 대한 평가

1. 현행의 집행체계와 그 한계

공공부문과 민간부문에서 개인정보보호원칙의 준수 여부를 실효성 있고 일관되게 감독하고 집행하며 효과적인 권리구제를 도모할 전문적이고 독립적인 감독기구의 존재가 필수적이고 시급하다. 그러나 현행 우리나라 개인정보보호기구들은 이러한 요청을 충족하지 못하는 한계를 가지고 있다.

(1) 첫째, **부문별로 부분적인 영역에서만 보호기구가 존재**하기 때문에 포괄적인 보호체계를 갖추고 있지 못하며, 따라서 많은 영역이 보호체계의 밖에 놓여 있다. 그나마 과거의 정보통신부(현재는 행정안전부 및 방송통신위원회) 산하의 개인정보침해신고센터와 개인정보분쟁조정위원회의 노력을 제외한다면, 다른 기관들은 개인정보보호기구로서의 기능을 거의 하지 못하고 있다고 해도 과언이 아니다. 지난 2002년과 2003년에 일어났던 교육행정정보시스템(NEIS) 사태[20]에서도 보는 바와 같이, 그 엄청난 사회적 갈등을 야기한 개인정보처리시스템의 구축과정에서도 「공공기관의 개인정보보호에 관한 법률」상의 주무부처였던 당시의 행정자치부와 개인정보보호심의위원회의 보호기능은 전혀 작동되지 않았다.[21]

---

20) NEIS는 2001년에 당시 교육인적자원부가 법률의 근거 없이 추진하였던, 초·중·고등학교의 학생정보를 비롯한 모든 교육행정정보를 통합시키는 전국단위 교육행정정보시스템(National Education Information System)을 가리킨다.

21) 참여연대가 2003년에 당시의 행정자치부에 개인정보보호심의위원회의 활동 내역에 대해 정보공개를

보호기구를 넓게 정의하여 법률에 명시적인 보호기관으로 지정되지 않더라도 실질적으로 보호기능을 수행하는 기관까지 포함한다면, 현재의 보호기구는 다음 표와 같다.

[표 1] 공공부문 개인정보보호기구 현황

기관명	근거법률	관할범위	주요 기능	특징
행정안전부 장관	「공공기관의 개인정보보호에 관한 법률」	공공기관 보유 개인정보	· 개인정보DB 보유 사전협의/공고 · 자료제출요구 및 실태조사 · 권리침해 신고접수·사실확인·확인결과통보·신고인에게 통지 · 공공기관에 의견제시 및 권고	· 일반행정기관(독임제) · 비전문성/비독립성 · 전자정부추진기관
공공기관개인정보보호심의위원회	상동	상동	· 정책 및 제도개선 사항 심의 · 개인정보 이용/제공에 대한 공공기관간의 의견조정 사항 심의 · 행전안전부장관이 요청하는 사항 심의 · 목적 외 이용/제공에 대한 심의	· 국무총리 산하 (위원장: 행안부차관) · 심의기구 · 비전문성/비독립성
교육과학기술부장관/교육감	「초·중등교육법」	교육정보	· 필요시 감독	· 교육정보시스템의 구축·운영자
국가인권위원회	「국가인권위원회법」	인권침해 일반	· 법령/제도/정책/관행 조사/연구 및 개선권고/의견표명 · 인권침해/차별 조사/구제 · 인권상황 실태조사/교육/홍보 · 지침의 제시/권고	· 일반인권 보호기구 · 독립성/비전문성 · 최근 정보인권침해조사/구제기능 강화

청구한 결과에 따르면, 1998년에서부터 2002년까지 5년 동안 3차례 회의가 열렸으며, 그 중 2차례는 서면심의로 진행되었고, 5년간 정식 회의 개최는 단 1차례에 불과했던 것으로 밝혀진 바 있다.

[표 2] 민간부문 개인정보보호기구 현황

기관명	근거법률	관할범위	주요 기능	특징
방송통신위원회	「정보통신망 이용촉진 및 정보보호 등에 관한 법률」	정보통신서비스제공자의 서비스제공과 관련한 이용자의 개인정보	· 법위반사실의 조사(자료제출요구/현장검사) · 법위반행위에 대한 시정명령 · 과징금 부과/징수 · 과태료 부과/징수 · 개인정보보호기술 개발/보급	· 방송통신 분야 정책/집행기관 · 대통령 산하 독립규제위원회 · 비전문성(개인정보) · 행정안전부장관과 정책/집행권한 중복 · 정보통신망의 이용촉진과 개인정보보호에 관한 정책과 집행을 함께 수행
	「위치정보의 보호 및 이용 등에 관한 법률」	위치정보	· 위치정보사업 허가 · 위치기반서비스사업 신고접수 · 과징금 부과/징수 · 과태료 부과/징수 · 분쟁에 대한 재정	· 위치정보의 이용과 보호에 관한 정책과 집행을 함께 수행
행정안전부장관	「정보통신망 이용촉진 및 정보보호 등에 관한 법률」	오프라인사업자(일부)의 서비스제공과 관련한 이용자의 개인정보	· 법위반사실의 조사(자료제출요구/현장검사) · 법위반행위에 대한 시정명령 · 과태료 부과/징수 · 개인정보보호기술 개발/보급	· 일반행정기관(독임제) · 비전문성/비독립성 · 방송통신위원회와 정책/집행권한 중복
개인정보 침해 신고센터	「정보통신망 이용촉진 및 정보보호 등에 관한 법률」	정보통신망법상의 개인정보	· 상담 및 고충처리 (법위반사실조사/자료제출요구) · 교육/홍보/연구 · 기술적 자문/지원	· 한국인터넷진흥원 소속 · 행안부와 방통위의 법집행보조기구
개인정보분쟁조정위원회	정보통신망법/위치정보법	정보통신망법/위치정보법상의 개인정보	· 분쟁조정신청 접수 · 사실조사/합의권고 · 조정(당사자의견청취/증거수집/전문가자문/조정결정)	· 행정안전부 산하 (장관이 위원 임명) · 위원(10명) 중 상임위원 1명 · 전문성 약화
금융위원회	「신용정보의 이용 및 보호에 관한 법률」	신용정보	· 신용정보업 허가/인가/등록 · 신용정보처리기준 제정 · 상담 및 피해구제 · 시정 권고 및 명령 · 과태료 부과/징수	· 국무총리 소속 중앙행정기관 · 금융정책/감독 총괄 · 신용정보의 이용과 보호에 관한 정책과 집행을 함께 수행 · 특정금융거래정보를 이용/보고하는 금융정보분석원을 산하에 둠 · 개인정보보호기구로 보기 어려움

(2) 둘째, 현재의 보호기구는 독립성과 전문성이 매우 취약하다. 현재 공공부문에서 개인정보보호의 주무부처는 행정안전부장관이다. 그러나 행정안전부장관은 동시에 전자정부를 추진하는 주무부처이다. 전자정부의 효율적 추진에 있어서는 개인정보의 이용의 가치가 우선할 수밖에 없다. 서로 상반되는 가치를 단일의 기관이 동시에 추진하면서 조화를 도모한다는 것이 전혀 불가능한 일은 아니지만 결코 쉬운 일은 아니다. 어느 한 쪽에 경도될 수밖에 없다.

한편, 현재 민간부문의 개인정보보호를 위한 집행체계는 매우 혼란스러울 뿐만 아니라 독립성과 전문성을 충분히 확보하고 있지 못하다. 현 정부가 들어서면서 기존의 정보통신부가 폐지됨에 따라 정보통신망법상의 개인정보보호에 관한 정책 및 집행기능이 방송통신위원회와 행정안전부장관에게 양분되어 분할되었다. 정보통신서비스제공자의 서비스제공과 관련한 이용자의 개인정보는 방송통신위원회가, 그 밖의 일부 오프라인사업자의 서비스제공과 관련한 이용자의 개인정보는 행정안전부장관이 맡고 있다. 그러면서도 온라인과 오프라인 양 부문의 분쟁조정기능을 수행하는 개인정보분쟁조정위원회는 행정안전부 산하에 있으면서 그 사무국을 인터넷진흥원에 두고 있고, 인터넷진흥원에 소속된 개인정보침해신고센터는 방송통신위원회와 행정안전부장관의 법집행보조기구로 기능하고 있다. 매우 기형적인 집행체계가 아닐 수 없다.

한편, 온라인 부문의 경우 개인정보보호에 관한 정책과 집행기능을 방송통신위원회가 맡고 있는데, 과거의 정보통신부에 비하면 방송통신위원회가 훨씬 더 보호기능의 중립성과 독립성을 확보할 수 있다는 점에서 보다 나은 측면이 있다. 과거의 정보통신부는 기본적으로 정보통신기반의 구축과 정보통신산업을 활성화하는 주된 임무를 맡고 있었기 때문에, 개인정보의 이용과 보호의 가치를 균형 있게 조정하기 어려운 측면이 있었다. 그럼에도 불구하고 아이러니컬하게도 과거의 정보통신부는 여론에 민감한 중앙행정기관으로서, 보호의 가치에 지나치게 치우친 매우 강력한 보호법의 제정을 주도했으며 그에 근거하여 사전예방적 감독기능이 아닌 사후집행 및 처벌 위주의 기능을 수행하였다. 이 과정에서 개인정보 이용의 가치는 온라인 부문에서 거의 사장되었으며 현재도 그러하다. 그 원인은 전문성의 부족에 있었던 것이 아닌가 생각된다. 개인정보보호 업무는 개인정보의 이용과 보호의 미묘한 균형을 아주 세밀하게 맞추어 내어야 하는 전문영역이다. 순환보직제가 적용되는 관료집단인 정보통신부로서는 이러한 전문성을 확보하는

것이 매우 어려운 일이 아닐 수 없다. 이 같은 전문성 확보의 난점은 현재의 방송통신위원회도 동일하게 부닥치는 문제이다. 방송통신위원회가 중립성과 독립성은 확보하고 있다 하더라도 개인정보보호 업무를 전담하는 기구가 아니기 때문이다.

(3) 셋째, 현재의 각 보호기구는 그 기능과 역할이 상당히 제한적이다. 가장 활발하게 보호기능이 작동하고 있다고 할 수 있는 정보통신 부문에서도, 그 보호기능은 주로 정보주체의 구제신청을 접수받아 사실조사를 행하고 그 결과에 기초해서 행정제재(과태료 부과) 또는 형사고발 조치를 취하거나, 민사배상에 대한 조정역할을 수행하는 데 머물러 있다. 예방적이고 사전적인 감시기능, 자율규제의 조정기능, 집단적인 대규모 침해에 대한 구제기능 등을 수행하지는 못 하고 있다. 특히 신용정보와 금융거래정보의 경우 금융위원회가 일정한 감독기능을 수행하는 것으로 법에서는 예정되어 있으나, 전담기구가 아니기 때문에 그 전문성이 떨어질 뿐만 아니라 신용정보와 금융거래정보의 이용정책도 동시에 추진하기 때문에 개인정보감독기구로서 한계가 있다.

2. 국회 제출 3개 법안의 집행체계의 내용

정부안	· 행정안전부장관이 공공과 민간부문 정책/집행/감독기능 포괄적 수행 - 국회/법원/헌법재판소/중앙선관위 독자적인 보호기능 수행 - 방통위(온라인 부문)/금융위(신용정보) 각 개별법에 의한 정책/집행기능 수행 - 각 중앙행정기관장은 소관 민간부문에서 중복적으로 정책/집행기능 수행 · 국무총리 소속의 개인정보보호위원회 심의기능 수행 · 개인정보분쟁조정위원회 별도설치(행안부장관이 위원 임명; 사무국 인터넷진흥원 내) · 개인정보침해신고센터(인터넷진흥원 소속; 행안부와 방통위의 법집행보조기구)
	<행정안전부장관의 정책/집행/감독기능> · 개인정보보호기본계획(3년 단위) 수립 (각 중앙행정기관장은 1년 단위 시행계획 수립) · 표준개인정보보호지침 제정/권고 (각 중앙행정기관장은 소관분야 보호지침 제정/권고) · 자율규제의 촉진 및 지원(교육/홍보, 보호단체 육성/지원, 인증마크 및 자율규약 지원) · 공공기관의 개인정보DB 등록/공개/개선권고 · 공공기관의 개인정보영향평가 관리 · 개인정보보호에 영향을 미치는 내용이 포함된 법령과 조례에 대한 의견제시 · 개인정보처리실태의 개선권고(각 중앙행정기관장은 소관분야 개선권고) · 권리침해신고 접수/처리 (개인정보침해신고센터가 수행) · 법위반사실의 조사(자료제출요구/현장검사)(각 중앙행정기관장 소관분야 조사) · 법위반행위에 대한 시정명령(국회 등에는 권고)(중앙행정기관장 소관분야 시정명령) · 법위반행위에 대한 형사고발/관련자 징계권고)(중앙행정기관장 소관분야 징계권고) · 과태료 부과/징수 (중앙행정기관장 소관분야 과태료 부과/징수)

이혜훈 의원안	· 국무총리 소속의 개인정보위원회가 독립적으로 공공과 민간부문 정책/감독기능 수행 – 보호와 이용의 균형적 발전을 강조하기 위하여 “개인정보위원회” 명칭 사용 – 위원회 주요 기능을 상담/피해구제, 교육/홍보, 기술개발지원, 제도개선에 둠 – 자료제출요구권, 실태조사권, 방문조사권, 시정권고, 시정명령, 고발/징계권고권 · 개인정보위원회에 개인정보분쟁조정위원회를 둠
변재일 의원안	· 대통령 소속 개인정보보호위원회가 독립적으로 공공과 민간부문 정책/감독기능 수행 – 보호와 이용의 균형을 도모 – 자료제출요구권, 실태조사권, 방문조사권, 시정권고, 시정명령, 고발/징계권고권 · 개인정보보호위원회에 개인정보분쟁조정위원회를 둠

3. 정부안의 집행체계에 대한 평가

(1) 정부안의 집행체계 옹호론

독임제 중앙행정기관인 행정안전부장관이 포괄적인 정책/집행/감독기능을 수행하는 방식의 정부안을 옹호하는 입장에서는 독립성·공정성의 확보에 있어서는 다소 문제가 있을 수 있으나, 책임성·신속성·강력한 집행력을 담보할 수 있다는 점에서 장점이 있다고 한다. 즉 정부행정조직의 일관성 있는 정책집행 및 협조와 지원, 효율적이고 신속한 피해구제, 강력한 법집행력 확보, 개인정보보호체계와 정보보호체계의 연계가능성 등을 장점으로 제시하고 있다.[22)]

또한 “다수의 위원으로 구성되는 위원회 체계는 상대적으로 시간을 가지고 신중하게 처리해야 하는 규제와 조정에는 합리적이나 개인정보 기본계획 등 진흥정책을 수립하여 집행하거나 위기에 신속하게 대응하여 의사결정을 하기에는 미흡할 수 있으며, 조직적인 측면에서 많은 공무원 인력을 유지할 수 없을 뿐 아니라 인사의 탄력성을 기하기도 어려운 현실적인 문제가 있다.”는 지적이 있다.[23)]

요컨대, 개인정보보호 업무는 개인정보의 유출, 오·남용 방지와 침해 시 즉각적인 대응을 위한 강력한 집행력 담보가 필수적이고, 특히 법률 시행 초기에는 강한 집행력에 근거한 개인정보보호 인식 제고와 보호체계 확립이 필요하기 때문에 정부안이 바람직하다

22) 국회 행정안전위원회가 2009. 4. 23. 개최한 「개인정보보호법안」에 대한 공청회에서 행한 염흥열 교수의 진술(공청회 자료집, 3-4면) 참조.

23) 국회 행정안전위원회가 2009. 4. 23. 개최한 「개인정보보호법안」에 대한 공청회에서 이상직 변호사가 행한 진술(공청회 자료집, 24-25면) 참조.

는 입장이다.

(2) 정부안에 대한 비판적 분석

그러나 정부안은 몇 가지 중요한 결함을 지니고 있는 것으로 보인다.

첫째, 상충되는 가치를 단일의 행정기관에게 동시에 추구하라고 요구하는 것은 무리한 요구이다. 행정안전부장관은 전자정부를 추진하는 주무부처이다. 전자정부의 효율적 추진에 있어서는 개인정보의 이용의 가치가 우선할 수밖에 없다.

특히 우리의 전자정부 이념은 행정의 효율성 가치에 경도되어 개인정보보공동이용을 전면적으로 추진하고 있다. 「전자정부법」은 개인정보공동이용을 전자정부의 핵심개념으로 상정하고 있고, 정부도 행정정보공유추진위원회와 행정정보공동이용센터를 설치해 범정부적 차원에서 적극적으로 추진해 나가고 있다.[24] 행정정보공유추진위원회가 설정하고 있는 행정정보공동이용체계의 기본방향과 행정정보공유센터의 역할과 기능에 의하면, 각 행정기관이 보유하고 있는 개인정보DB와 기업정보DB를 통합 연계하는 것을 기본전제로 하고 있다. 그러나 정부가 국민의 개인정보와 기업의 정보를 통합할 수 있는 가능성을 열어 두는 것 자체는 자유민주주의체제에서 경계해야 될 일이다. “개인정보공동이용”을 전자정부의 핵심개념이자 기본전제로 여기는 사고는 정부기능의 효율성만을 강조한 것으로서 행정의 민주성과 투명성의 가치를 경시한 것이라고 평가하지 않을 수 없다.

이런 상황에서 행정안전부장관이 충돌하는 양 가치의 균형을 적정하게 이루면서 개인정보보호정책을 수립하고 이를 충실하게 집행해나가는 것이 비록 불가능하지는 않다 하더라도 지극히 어려운 일임에 틀림없다. 더 나아가, 행정안전부장관은 그 자신이 개인정보처리기관으로서 주민등록정보DB, 지적정보DB 등을 구축·보유하고 있을 뿐만 아니라 많은 다른 기관들과 개인정보를 상호 공유하고 있다. 행정안전부장관 자신이 감독을 받아야 하는 대상기관인 것이다. 이는 ‘누구도 자신의 사건에 재판관이 될 수 없다’는 자연적 정의에 반한다.

둘째, 행정안전부장관은 중앙의 행정부처로서 독립성과 중립성을 담보하기 어렵다.

24) 행정정보 공동이용의 추진과정과 상황에 관해서는 행정정보공유추진위원회가 2007년 12월에 발간한 『2007 행정정보공동이용 백서』, 24-140면 참조.

장관은 정무직 공무원으로서 임기의 보장이 없으며 정치적 상황에 따라서는 매우 단명으로 끝나기도 한다. 특히 우리나라의 경우 장관직은 그 생명이 매우 짧다. 수시로 바뀌는 장관에 의해서는 일관된 정책이 유지되기 어렵다.

셋째, 행정안전부장관은 개인정보보호를 전담하는 기관이 아니며 때문에 전문성이 결여되어 있다. 「정부조직법」상 행정안전부는 중앙행정기관의 하나로서 공무원의 인사·복무·연금, 상훈, 정부혁신, 전자정부, 지방자치제도, 지방자치단체의 사무지원·재정·세제, 선거, 국민투표, 안전관리정책 및 비상대비·민방위·재난관리 등 다양한 업무를 수행하고 있다. 결코 개인정보보호를 위한 전문기관이라고 볼 수 없다. 개인정보보호를 담당하는 공무원도 순환보직제로 인해 전문성을 확보하지 못한다. 개인정보보호 업무는 개인정보의 이용과 보호의 미묘한 균형을 아주 세밀하게 맞추어 내어야 하는 전문영역이다. 장관도 담당공무원도 전문성이 없는 상태에서 전문적인 개인정보보호 업무를 일관되게 객관적으로 추진하기를 기대하는 것은 무리이다.

넷째, 정부안은 행정안전부장관, 개인정보보호위원회, 분쟁조정기구, 침해신고센터가 각각 분리되어 기능하고 있어 오히려 효과적인 보호정책과 감독기능을 수행하기 어렵도록 되어 있다. 또한 민간부문의 경우 행정안전부장관과 각 중앙행정기관장이 중첩적으로 집행권한을 행사하도록 되어 있다. 더 나아가, 온라인 부문과 신용정보 부문에서는 방송통신위원회와 금융위원회가 현재와 같은 문제점을 그대로 안은 채 소위 보호기능을 수행하도록 예정되어 있다. 결국 국가 전체적으로 통일되고 체계적이며 일관된 정책·집행·감독기능을 수행하기 어렵도록 되어 있다.

다섯째, 마지막으로 우려되는 바는, 공공부문과 민간부문의 집행에 있어서 불균형이 심화되지 않을까 염려된다. 현재도 공공부문에 대한 감독기능은 현저히 약화되어 있고, 반면에 민간부문에서는 매우 강력한 사후처벌 위주의 집행체계가 구축되어 있다. 정부안은 이러한 현상을 더욱 심화시킬 것으로 보인다. 정부안의 개인정보처리기준은 특히 민간부문의 경우 일반법으로서는 세계에서 보기 드물 정도로 매우 강한 보호기준으로 되어 있다. 자칫 민간부문에서 필요로 하는 개인정보의 이용을 과도하게 억제하고 그로 인해 민간의 경제적 활력이 약화되지 않을까 우려된다. 선진 각국의 개인정보보호체계가 왜 사후처벌이 아닌 사전예방적 감독기능에 초점을 맞추고 있는지 그 뜻을 헤아려야 할 것이다.

VI. 질의사항

Graham Greenleaf 교수님과 Marie GEORGES 자문관님에게 몇 가지 의문사항에 대한 질의를 드리고자 한다.

1. 호주나 유럽에서 개인정보감독기능을 국가인권기구가 아닌 별도의 개인정보감독기구에게 맡기는 이유가 무엇인가? 호주의 개인정보감독기구는 처음에는 국가인권기구 소속 하에 있다가 2000년 7월 1일부터 독립된 기관으로 분리되어 활동하고 있는데, 그 배경과 이유는 무엇인가?
2. 호주나 유럽에서 전자정부를 추진함에 있어서 “개인정보 공동이용의 원칙”을 채택하고 있는가? 공공기관이 보유하는 개인정보DB를 연계·통합하는 시도가 있는가?
3. 호주나 유럽의 개인정보감독기구는 법위반행위에 대하여 직접적인 시정명령을 내리거나 제재(과징금이나 과태료)를 부과하는가?
4. 호주나 유럽의 개인정보감독기구는 개인정보의 “이용”과 “보호”를 어떻게 조화시키는가?

개인정보보호감독기구의 위상과 역할에 관한 토론문

이항우 (충북대 사회학과)

3
토 론

For discussion on the role and position of the authorities protecting personal information

Lee, Hang-Woo
(Professor at Department of Sociology, Chungbuk National University)

I.

The presentations by Ms. Marie Georges and Mr. Graham Greenleaf analyze the data protection policies in Europe and the Asia-Pacific region and consider the social role of data protection institutions, independence requirements and a supervisory system covering both the public and private sector and the need to combine with other human rights functions. As Mr. Greenleaf says in his paper, there is a growing need, especially in this information society, to establish and operate independent data protection authorities which are governed by a law, not by an executive order or delegated legislation, retain ability to conduct independent investigations, have a fixed term of office for its members, cover both the public and private sector and are free from the pressures from administrative powers.

II.

In this light, the institutional protections in Korea lag far behind those in Europe and many other countries of the world which are governed by a comprehensive law applicable to both the public and private sector and provide for independent activities of the personal information protection authority. With regard to the laws and institutions to protect personal information, Korea has a general law "Public Agency Data Protection Act" for the public sector, but no such corresponding law for the private sector. Jlat like in the US, there are

many sectoral laws including ‘Use and Protection of Credit Information Act’, ‘Act on Real Name Financial Transactions and Guarantee of Secrecy’, ‘Protection and Communications Secrets Act’, ‘Act on Protection and Use of Location Information’ and 'Act on the Facilitation of Information-Communication Networks Use and the Protection of Personal Information' (‘AICN’). As an enforcement model for personal information protection, Korea has set up the Personal Information Commiaws an(PIC) which is supposed to handle public-sector theputes over personal information.n owever, the Commiaws a, which is currently tect of the Ministry of Public Administration and Security (MoPAS), has toooolittle to resthvas sose theputes. As for the activities related to the use and supply of information and telecommunications srrenc onthe oacys currently tbodd telforce is Commiaws aer for the Mediation of Conflict on Personal Information (CMCPI), which is also under the cont th of MoPAS and wsose oacys curment ientased on the ‘AICN’ of 2001. This Committee ommuntended to perform the theputes of on, Korea has a general law "P,s currentea hded use and mediatia hrelevant theputes. To sum up, Korea has no general law on ps a general lawtion protection to cover both the private and public sector, and there exists no independent authority for personal information protection, whether in the public or private sector. In order that this country may not remain underdeveloped any longer in the field of human rights on personal information, it is critical, as is stressed in Mr. Greenleaf's paper, to introduce a general law for personal information protection and establish an independent authority for personal information protection at the earliest possible.

III.

It is worthwhile to evaluate more positively the role of CMCPI for the past 8~9 years in making efforts to improve the situation of the information human rights in Korea. As is pointed out above, CMCPI is part of MoPAS and is clearly limited in that it simply handles the privacy violations arising in the activities relating information and telecommunications

services. Still, it should be noted that CMCPI was established under the strong influence of the 1995 European Union 'Directives' and, accordingly, is partly an independent authority for personal information protection with the rights of independent supervision and investigation. Moreover, it is based on a law, not on an enforcement regulation or delegated legislation, its members have their term in office defined in the law and its performance is published in an annual report. The mediating activities of the Committee are carried out in the following way: The Committee, upon receiving an application for mediation on a dispute case which may be subject to the dispute mediation by CMCPI under AICN, shall notifyediatiparties of the dispute are carn embark on a fact-finding investigation to dn erminetion for the personal information right has bern violated. The investigation into factual aspects involves: hearing the statements from the applicant party, the other party and witnesses; collecting explanations and documentary evidence to support those statements; advice from relevant experts; and field investigation. After the fact-finding investigation, the Committee shall recommend both parties to reach a mutual agreement, before initiating a mediation process. If the parties succeed in reaching an agreement, the case is closed in an 'agreement before mediation', but if they fail to do it, the mediation process follows. Once the mediation process is initiated, the Committee shall draw up a mediator's proposal no later than 60 days from the date of application receipt and recommend the parties to accept it. If both parties accept the 'mediating decision' by the Committee, the dispute case is successfully mediated. If either of the parties reject the 'decision', the case shall be referred to civil proceedings or be dismissed. Table 1 below shows the number of dispute cases by year that the Committee had successfully mediated from 2002 to 2006: 56 cases in 2002; 55 in 2003; 75 in 2004; 63 in 2005 and 63 in 2006. These figures indicate that the Committee is a personal information protection institution with independence of some extent in legal standing, the right to investigate and enforcement power. What should be pursued in the future efforts to protect personal information are to improve the personal information protection system further, by enacting a general law on personal information protection covering both the public and private sector and creating a body independent of the government, in the light of the

experiences the Committee has accumulated.

Table 1. The number of major cases of dispute mediated by the Committee (2002～2006)

Year	Mediation decision	Agreement before mediation	Consumer counselling	Business counselling	Total
2002	16	40	0	0	56
2003	28	27	0	0	55
2004	37	9	14	14	74
2005	25	18	12	8	63
2006	23	23	6	0	52
Total	129	117	32	22	300

Source: Korea Internet & Security Agency (KISA) (2003; 2004a; 2004b; 2005; 2006)

IV.

I'd like to move to a question to which Ms. Georges and Mr. Greenleaf paid less attention while emphasizing the significance of an independent data protection institution: how effective the personal information protection laws are in the EU member states and other nations. We cannot expect that, in practice, a law protecting personal information will always put the rights of individual data subjects first, even at the expense of the interests of large companies or capitals, just because the personal information protection institution is guaranteed statutory independence. This is due to the fact that, in this information society, personal information is not only a core factor of the traditional human rights but also economic commodities or goods. As is implied in the titles of OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (‘Guideline’)" in 1980 and the EU “Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (‘Directive’)” in 1995, it is widely accepted today that personal

information is a factor of human rights which should be cherished and protected and, at the same time, an economic commodity which should be freely distributed. Personal information is no longer of an absolute value as a human right but should be also viewed in the light of its economic value. The problem here is that, in the market of personal information, the predominant power is in the hand of the data processors, that is, the capital, not of individual data subjects. Namely, there is a high likelihood that the value of personal information as commodities is put before its value as a human right. The legislative independence of personal information protection authorities, which is stressed throughout the papers by Ms. Georges and Mr. Greenleaf, is not, in itself, a necessary and sufficient condition to resolve this mismatch.

V.

It is important to ensure that, in the course of actual enforcement of a data protection law by an independent data protection authority, 'the fair information principle' is fulfilled. In other words, it is critical that the data protection authority should be independent of the market power, as well as of the government power. For instance, how effective is the practical application of the principles that 'personal information may be collected only in a legal manner and on the consent of the data subject' and 'disclosure of data should be in compliance with the initial purpose of data collection'? In Korea, these principles are reflected in the provisions of the AICN banning 'data collection without consent of data subjects' and 'use of data for purposes beyond the consented scope'. In reality, however, the disputes between data collectors and data subjects, which are handled by CMCPI on the basis of those principles and law provisions, are more concerned about illegal activities associated with the data than about the collection of data itself without consent of the data subject. In this situation, it is ambiguous whether the sanction against a particular data controller is for his/her collection of data without consent of the data subject or for other illegal activities

using the data. In practice, all of the dispute cases for which CMCPI has given a mediation decision are related to the illegal activity of enlisting data subjects in the subscription of particular services without their consent, not to the data collection without consent in itself. In one example, a telephone service provider collected personal information of the data subjects without their consent and modified their phone bill payment method without their consent. Similar problems are detected in the actual application of the principle that 'personal information should be protected by way of proper devices designed to prevent unlawful access to the information and damage, modification and leakage of the information' and the provision of the AICN requiring 'destruction of personal information after the purpose of collection or receipt is accomplished'. According to the documents of Parliamentary inspection in 2003, the top three mobile service providers retained personal information of, respectively, 4,432,000, 3,426,000, and 2,958,000 persons even after their subscription had been terminated. A civic group filed a complaint demanding compensation for psychological damages, considering that the case constituted a contravention of the provision on destruction of personal information. But the complaint was dismissed, on the ground that 'such exemptions for the need to retain transactional data as are provided for in other laws, including the Commercial Law', are acknowledged. If such need to retain data under another law can reserve the effect of the provision on data destruction without delay, it is questionable whether it is a simple exemption. In reality, the requirement for 'data destruction without delay' takes effect without being reserved by such exemptions, mostly when a data processor has not destroyed personal data and used them illegally, such as the case where an Internet service provider used the data about its former subscribers to enlist them in another subscription of the provider. Then, in case a data processor keeps the data whose purpose of collection has been accomplished, instead of destroying them without delay, it is not certain that the data processor is punished under the AICN even if his/her guilt for an illegal activity using the data is not established. In brief, the principle of fair information, on which the OECD Guidelines and the AICN of Korea are based, may be construed as a dead rule in reality.

Table 2. Applications for damages in relation to personal information violations, by year and type (2002-2006) (in %)

Alleged violations	2002	2003	2004	2005	2006
Personal data collection without consent of data subjects	4.3	2.3	3.2	6.3	10.99
Excessive collection of personal data	0.1	0.2	0.2	0.1	0.12
Failure to comply with the obligations of notification or specification at the time of data collection	0.4	0.2	0.2	0.2	0.26
Use or disclosure of data for a purpose beyond the scope notified or specified	7.4	4.6	11.9	5.0	3.93
Damage/encroachment or leakage by the personal data processor	1.9	3.4	7.7	1.0	0.88
Failure to comply with the obligation of notification at the time of commissioning the personal data processing	0.0	0.2	0.0	0.05	0.02
Failure to comply with the obligation of notification on business transfer, etc.	0.1	0.0	0.0	0.05	0.05
Failure to designate a person responsible for personal data management	0.1	0.1	0.0	0.2	0.09
Insufficient technical and managerial measures to protect personal data	1.1	1.4	2.1	2.1	2.7
Failure to destroy personal data after the purpose of their collection or receipt is achieved	3.9	9.6	1.1	0.8	1.2
Failure to accept a request for consent cancellation, data inspection or correction	13.3	6.2	6.8	4.2	3.96
Failure to take actions to adopt easier methods for consent cancellation, data inspection or correction than for data collection	1.9	0.1	0.3	1.6	2.1
Collection of children's personal data without consent of their legal representative	61.3	66.4	33.2	0.4	0.1
Damage, encroachment or stealth of other peoples' personal data, including resident ID numbers	3.5	4.6	24.1	53.9	46.4
Others (credit information violations, infringement of job-related privacy and other types of violations not included in the ICN Act)	0.7	0.9	8.2	24.1	27.2
Total	**100**	**100**	**100**	**100**	**100**

Source: KISA (2003; 2004a; 2004b; 2005; 2006)

VI.

Last but not least, in relation to the significance of personal information as a human right value, it cannot be overemphasized that, as is also stressed by Ms. Georges, protecting personal information is not simply protecting privacy but protecting our fundamental rights, including the freedom of association, the freedom of religion and conscience, the freedom of expression, the freedom of information, human dignity and autonomy. Only when personal information is not seen as an object of easy commercial transaction but a fundamental right which is enshrined in the Constitution can we successfully achieve our goals of enacting a general law on personal information protection, establishing an independent authority for personal information protection and enforcing the right to self-determination of personal information effectively.

3
토 론

개인정보보호감독기구의 위상과 역할에 관한 토론문

이항우 (충북대 사회학과)

I.

조지와 그린리프의 발표문은 각각 유럽과 아시아의 데이터 보호 정책에 관한 분석을 통해, 데이터 보호 기구의 사회적 역할, 독립성 요건, 공적인 부문과 사적인 부문의 통합적 감시, 인권 보호 관련 기능과의 통합 필요성 등의 문제를 고찰하고 있다. 그린리프가 말한 바와 같이, 세계의 많은 나라들이 독립적인 데이터 보호 기구, 즉 시행령이나 위임입법이 아니라 법률에 의거하여 설립되고, 독자적인 조사권을 가지며, 위원의 임기가 법적으로 보장되며, 공적 부문과 민간 부문을 모두 포괄하는, 행정 권력으로부터 자유로운 독립적인 데이터 보호 기구를 설립하고 운영해야 필요성은 오늘날과 같은 정보화 시대에 점점 더 커지고 있다고 생각한다.

II.

이러한 관점에서 볼 때, 우선, 오늘날 한국의 개인정보 보호 제도는 유럽을 비롯한 세계 많은 나라들이 채택하고 있는, 공/사 부문 모두를 포괄하는 개인정보 보호법의 토대 위에서 개인정보 보호기구가 독립적인 활동을 할 수 있도록 보장하는 제도와는 한참 동떨어져 있다고 말할 수 있다. 개인정보 보호를 위한 법률 및 제도와 관련하여, 한국은 공공 부문에서는 '공공기관의 개인정보 보호에 관한 법률'이라는 일반법을 두고 있으며, 민간 영역에서는 그러한 일반법을 두고 있지 않다. 미국과 유사하게, 분야별로 '신용정보 이용 및 보호에 관한 법률', '금융실명거래 및 비밀보장에 관한 법률', '통신비밀보호

법', '위치정보의 보호 및 이용에 관한 법률', '개인정보 보호와 정보통신망 이용촉진에 관한 법' 등을 운용하고 있을 뿐이다. 그리고 개인정보 보호 집행모델과 관련하여, 한국은 공공 영역의 개인정보 분쟁을 담당하는 개인정보심의위원회를 두고 있다. 그러나 현재 행정안전부에 소속되어 있는 이 기구는 거의 아무 활동도 하지 않는 사실상 유명무실한 조직이다. 민간부문 중 정보통신서비스 제공 및 이용과 관련된 부문은 2001년 '정보통신망법'에 의거하여 만들어진 행정안전부 산하의 개인정보분쟁조정위원회가 개인정보 보호감독 및 분쟁조정 기능을 수행하고 있을 뿐이다. 요컨대, 한국은 공공 부문과 민간 부문을 포괄하는 개인정보 보호 일반법을 갖고 있지 않으며, 공공 부문과 민간 부문을 막론하고 개인정보 보호를 위한 독립적 기구를 운용하고 있지도 않다. 하지만 한국이 더 이상 정보인권 후진국에 머물러 있지 않으려면, 조지와 그린리프의 논의에서 볼 수 있듯이, 하루 빨리 개인정보 보호 일반법을 도입하고 개인정보 보호를 위한 독립기구를 설립하는 것이 필요하다.

III.

한국이 정보인권 선진국으로 나아가기 위한 노력에서 지난 8-9년 동안 '개인정보분쟁조정위원회'가 수행한 활동을 좀 더 적극적으로 평가할 필요가 있다. 물론, 앞에서 지적한 것처럼, 개인정보분쟁조정위원회는 행정안전부 소속 기관이며 정보통신서비스와 관련된 영역에서 발생하는 개인정보 침해문제를 다룬다는 명백한 한계를 지니고 있다. 하지만, 그것은 1995년 유럽연합 '지침'의 영향을 많이 받고 설립되었으며, 따라서 감시권한의 독립성과 독자적 조사권 보유라는 측면에서 독립적인 개인정보 보호 기구로서의 성격을 일부 지니고 있다. 개인정보분쟁조정원원회는 시행령이나 위임입법이 아닌 법률에 바탕을 두고 있으며, 독자적인 조사권을 갖고 있다. 위원들의 임기는 법률로 정해져 있으며, 위원회의 활동을 연간 보고서로 공개한다. 개인정보분쟁조정위원회 조정활동은 대체로 다름과 같은 방식으로 이루어진다. 분쟁조정위원회는 정보통신망법 상의 분쟁조정 대상이 되는 사안에 대하여 조정 신청이 접수되면, 신청인과 피신청인 모두에게 이 사실을 통보하고, 개인정보 침해여부를 판단하기 위한 사실조사에 착수한다. 사실조사

는 신청인과 피신청인 그리고 참고인의 진술 청취, 진술을 뒷받침할 수 있는 소명 및 입증 자료의 수집, 전문가 자문, 사건 현장 답사 등의 활동이 이루어진다. 사실조사 후 분쟁조정위원회는 본격적인 조정에 들어가기 전에 당사자 간 합의를 권고한다. 만일 원만한 합의가 이루어지면 사건은 '조정 전 합의'로 종결되지만, 합의가 이루어지지 않으면 본격적인 조정절차가 시작된다. 조정절차가 시작되면 분쟁조정위원회는 분쟁조정 신청일로부터 60일 이내에 조정안을 작성하여 신청인과 피신청인에게 그에 대한 수락을 권고한다. 분쟁조정위원회의 '조정 결정'을 양 당사자가 수락하면 조정이 성립되지만, 당사자 중 어느 한쪽이 거부하면 조정절차는 종료되고 사건은 민사소송으로 넘어가거나 혹은 취소될 수 있다. 실제로 개인정보분쟁조정위원회는 아래의 <표-1>에서 볼 수 있는 바와 같이, 2002년에는 56건, 2003년에는 55건, 2004년에는 75건, 2005년에는 63권, 2006년에는 52시의 분쟁을 조정하였다. 이처럼 개인정보분쟁조정위원회는 조직의 법률적 지위, 조사권, 집행력 등에서 일정한 독립성을 지닌 개인정보 보호 기구라 할 수 있다. 한국의 정보보호 노력이 앞으로 해야 할 과제는, 이러한 개인정보분쟁조정위원회의 경험을 바탕으로, 공/사 부문을 모두 포괄하는 개인정보 보호 일반법을 제정하고, 정부로부터 독립적인 개인정보 보호 기구를 설치하여, 개인정보 보호 시스템을 더욱 선진화하는 일이다.

<표-1> 개인정보분쟁조정위원회의 주요 분쟁조정 사례 건수(2002~2006)

유형/년도	조정결정	조정 전 합의	소비자 상담	기업 상담	합계
2002	16	40	0	0	56
2003	28	27	0	0	55
2004	37	9	14	14	74
2005	25	18	12	8	63
2006	23	23	6	0	52
합계	**129**	**117**	**32**	**22**	**300**

* 출처: 한국정보보호진흥원(2003; 2004a; 2004b; 2005; 2006)

IV.

다음으로, 조지와 그린리프가 독립적 데이터 보호 기구의 중요성을 강조하느라 상대적으로 소홀하게 다룬 문제가 있다. 그것은 유럽연합 국가들을 비롯한 각국의 개인정보 보호 제도의 실효성에 관한 것이다. 개인정보 보호 기구가 법적인 독립성을 보장받는다고 해서, 개인정보 보호 법률의 실제 집행에서 그것이 반드시 대기업이나 대자본의 이익에 반하여 개별 정보 주체의 권리를 우선시할 것이라고 기대할 수는 없다. 이러한 문제는 오늘날과 같은 정보화 사회에 개인정보란 전통적인 인권의 핵심요소이기도 하지만 동시에 하나의 경제적 재화 혹은 상품이기도 하다는 사실에 기인한다. 경제협력개발기구(OECD)의 1980년 '프라이버시 보호와 국가 간 개인정보의 자유로운 흐름을 위한 가이드라인'이나 유럽연합(EU)의 1995년 '개인정보와 연관된 개인의 보호 및 개인정보의 자유로운 흐름에 관한 지침'이라는 명칭에서도 알 수 있듯이, 오늘날 개인정보는 우리가 소중하게 다루고 보호해야 하는 인권의 한 요소이기도 하지만 동시에 자유롭게 유통해야 하는 경제적 재화이기도 하다는 인식이 널리 퍼져 있다. 이제 인권으로서의 개인정보는 더 이상 절대적 가치가 되지 못하고, 그것이 가진 경제적 가치와 항상 균형을 맞추어야 하는 것이 되어 버린 셈이다. 그런데 문제는 개인정보를 둘러싼 오늘날의 시장상황에서 지배적인 힘을 행사하는 주체는 개별 정보 주체라기보다는 정보 처리 주체 즉 자본이라는 사실이다. 즉, 개인정보가 가친 인권적 가치보다 상품적 가치가 우선시될 현실적 가능성이 훨씬 높다는 것이다. 그런데 조지와 그린리프가 말한 개인정보 보호기구의 법률적 독립성 자체는 이러한 불균형을 바로잡을 수 있는 필요충분조건이 되지 못한다.

V.

독립적 데이터 보호 기구에 의한 데이터 보호 법률의 실제 집행과정에서 이른바 '공정한 정보 원리'가 실질적으로 관철되도록 만드는 것이 중요하다. 다시 말해서, 데이터 보호 기구가 국가권력뿐만 아니라 자본으로부터도 실질적으로 독립하는 것이 중요하다. 예를 들어, '합법적으로 그리고 정보주체의 동의 하에 필요한 개인정보만을 수집해야 한

다'는 원리와, '개인정보 수집 목적과 일치하도록 정보공개가 이루어져야 한다'는 원리는 현실적으로 얼마나 실효성 있게 관철되는가? 한국의 경우, 그러한 원리들은 정보통신망법에서 '동의 없는 개인정보 수집 금지'와 '동의의 범위를 넘어선 개인정보 이용 금지'라는 법률조항들에 반영되어 있다. 그런데 분쟁조정위원회가 이러한 원리와 법률조항에 근거하여 정보수집자와 정보주체 사이의 분쟁을 조정하는 사례들은 동의 범위를 벗어난 이용 그 자체보다는, 그것들이 다른 불법적 활동과 연관된 경우들이 거의 대부분을 차지하고 있다. 이런 경우, 정보처리 주체에 대한 처벌에 과연 개인정보의 동의 없는 수집에 대한 것인지 혹은 그것의 또 다른 불법 활동에 대한 것인지 모호해진다. 실제로 분쟁조정위원회가 조정 결정을 내린 모든 동의 없는 개인정보 수집 관련 사례들은, 순수한 동의 없는 수집 그 자체보다는 그 정보를 이용하여 정보주체를 특정 서비스에 무단으로 가입시키는 활동과 연관되어 있다. 이를테면, 전화 사업자가 정보주체의 개인정보를 동의 없이 수집하여, 그 사람의 전화요금 납부 방법을 무단으로 변경시키는 경우가 그 예에 해당한다. 이러한 문제는 '개인정보는 불법적 접근, 훼손, 변경, 누설 등을 예방하기 위한 적절한 장치에 의해 보호되어야 한다'는 원리와 '수집 또는 제공받은 목적 달성 후 개인정보의 파기'라는 국내 정보통신망법의 법률규정의 실제 적용에서도 드러난다. 2003년 국정감사 자료에 따르면, 국내의 주요 이동통신사업자 3사가 개인정보를 계속 보유하고 있는 해지고객의 수는 각각 443만 2천명, 342만 6천명, 295만 8천명에 이르는 것으로 나타났다. 그러나 이 사례가 목적 달성 후 개인정보 미파기에 해당한다고 본 시민단체의 정신적 피해보상 요구는 예외 조항, 즉 상법 등 '다른 법령에 의한 상거래 자료의 보존과 같은 보존 필요성'이 인정될 수 있다는 조항 때문에 기각되었다. 그러나 다른 법령에 의한 자료 보존의 필요성 인정이 지체 없는 파기를 이런 식으로 유보시킬 수 있다면, 그것을 단순한 예외 조항으로 볼 수 있을지 의심스럽다. 실제로 '지체 없는 파기'가 이와 같은 예외 조항에 의해 유보되지 않고 효력을 발생하는 경우는, 예를 들어 인터넷 서비스 사업자가 서비스 탈퇴회원에 대한 정보를 이용하여 자사의 또 다른 서비스에 무단으로 가입시키는 것과 같이, 미파기한 개인정보를 불법적으로 사용한 경우들이 대부분이다. 그러면 과연 수집 목적을 달성한 개인정보를, 그 불법적 활용이 분명히 드러나지 않는 한, 즉각 파기하지 않고 계속 보관하는 것은 현실적으로 정보통신망법의 실질적인 처벌 대상이 된다고 말할 수 있을지 의문이다. 요컨대, OECD 가이드라인과 한

국의 정보통신망법의 토대가 되는 '공정한 정보원리'가 제도의 실제 운영에서는 사실상 사문화된 규칙으로 이해될 수 있는 여지가 너무나도 많다고 말할 수 있다.

<표-2> 2002-2006 연도별·유형별 개인정보 피해구제 신청현황(%)

침해유형	2002	2003	2004	2005	2006
이용자 동의 없는 개인정보 수집	4.3	2.3	3.2	6.3	10.99
과도한 개인정보 수집	0.1	0.2	0.2	0.1	0.12
개인정보 수집시 고지 또는 명시 의무 불이행	0.4	0.2	0.2	0.2	0.26
고지·명시한 범위를 초과한 목적외 이용 또는 제3자 제공	7.4	4.6	11.9	5.0	3.93
개인정보 취급자에 의한 훼손·침해 또는 누설	1.9	3.4	7.7	1.0	0.88
개인정보 처리 위탁시 고지의무 불이행	0.0	0.2	0.0	0.05	0.02
영업의 양수 등의 통지의무 불이행	0.1	0.0	0.0	0.05	0.05
개인정보 관리책임자 미지정	0.1	0.1	0.0	0.2	0.09
개인정보보호의 기술적·관리적 조치 미비	1.1	1.4	2.1	2.1	2.7
수집 또는 제공받은 목적 달성 후 개인정보 미파기	3.9	9.6	1.1	0.8	1.2
동의철회·열람 또는 정정 요구 불응	13.3	6.2	6.8	4.2	3.96
동의철회·열람·정정을 수집방법보다 쉽게 해야 할 조치 미이행	1.9	0.1	0.3	1.6	2.1
법정대리인의 동의 없는 아동의 개인정보 수집	61.3	66.4	33.2	0.4	0.1
주민번호 등 타인 정보의 훼손·침해·도용	3.5	4.6	24.1	53.9	46.4
기타(신용정보 침해, 직장프라이버시 침해 등 정보통신망법 규정 외의 침해유형)	0.7	0.9	8.2	24.1	27.2
합계	**100**	**100**	**100**	**100**	**100**

* 출처: 한국정보보호진흥원(2003; 2004a; 2004b; 2005; 2006)

VI.

마지막으로, 개인정보가 가진 인권적 가치의 중요성과 관련하여, 조지가 말한 것, 즉 개인 정보 보호가 단순히 프라이버시 보호를 넘어서서, 결사의 자유, 종교와 양심의 자유, 표현의 자유, 정보의 자유, 인간 존엄성과 자율성 등과 같은 우리의 근본적 권리를 보호하는 것이 된다는 지적은 매우 아무리 강조해도 지나치지 않은 것이라고 생각한다. 우리의 개인정보를 손쉬운 경제적 거래 대상, 즉 상품으로 간주하는 것이 아니라, 그것이 지닌 헌법적인 근본적 인권의 가치를 충분히 이해할 수 있어야만, 개인정보보호감독기구의 역할과 관련한 우리의 과제, 즉 개인정보보호 일반법의 제정과 독립적인 개인정보보호감독기구의 설립, 그리고 개인정보자기결정권의 실효성 있는 적용이라는 과제를 성공적으로 달성할 수 있을 것이다.

국제심포지엄
: 개인정보보호감독기구의 역할과 위상

| 인 쇄 | 2009년 9월
| 발 행 | 2009년 9월

| 발행인 | **현 병 철**
| 발행처 | **국가인권위원회 인권정책과**
| 주 소 | (100-842) 서울특별시 중구 무교동길 41
금세기B/D (을지로1가 16번지)
| 전 화 | (02) 2125-9759 | F A X | (02) 2125-9733
| Homepage | www.humanrights.go.kr

| 인쇄처 | 도서출판 **한학문화**
| 전 화 | (02) 313-7593 | F A X | (02) 393-3016

발간등록번호 11-1620000-000180-01

사전승인 없이 본 내용의 무단복제를 금함

국제심포지엄

개인정보보호감독기구의 역할과 위상

International Symposium on the Role and Position of an Institution Protecting Individual Privacy

국가인권위원회
National Human Rights Commission of Korea

(우)100-842 서울시 중구 무교동길 41 금세기 빌딩 11층(을지로 1가 16)
전화: 02) 2125-9759, 팩스: 02) 2125-9733 www.humanrights.go.kr