2025
제14회 한국인터넷거버넌스포럼(KrIGF)
결과 보고서

2025. 09.

한국인터넷거버넌스포럼 프로그램위원회

목 차

0. 한국인터넷거버넌스포럼(KrIGF) 소개

인터넷거버넌스포럼(Internet Governance Forum, IGF)은 정부, 기업, 시민사회, 학계, 기술 커뮤니티, 이용자 등 다자간(multi-stakeholder)의 정책 대화를 위해 만들어진 포럼입니다.

지난 2005년 개최된 정보사회세계정상회의(WSIS)의 결과 문서인 튀니스 어젠더(Tunis Agenda)의 72항에 따라 2006년 아테네에서 처음 개최되었으며, 이후 개최 국가를 달리하며 매해 개최되고 있습니다.

IGF는 인터넷 관련 공공정책 이슈와 관련하여 정부, 기업, 시민사회, 학계, 기술 커뮤니티, 국제기구 등 다양한 이해당사자 사이의 대화를 촉진하고, 새로운 인터넷 관련 이슈들이 제기되며, 개발도상국이나 새로운 참여자의 정책 역량을 강화하는데 큰 역할을 해온 것으로 평가되고 있습니다.

한편, IGF는 단순히 정책토론에 그치는 것이 아니라, 주요 인터넷 관련 정책 이슈에 대해 '권고' 등 보다 구체적인 결과물을 생산할 것을 요구받고 있습니다.

지난 2014년 4월 23~24일 상파울루에서 개최된 넷문디알(NetMundial) 회의(인터넷 거버넌스의 미래에 대한 멀티스테이크홀더 회의)에서도 IGF의 강화 필요성을 다시 한 번 권고한 바 있습니다.

한국 인터넷거버넌스포럼(KrIGF)은 주요 인터넷 관련 공공정책 이슈와 관련하여 정부, 기업, 시민사회, 학계, 기술 커뮤니티, 이용자 등 국내 다양한 이해당사자들 간의 대화와 토론을 촉진하는 것을 목적으로 합니다.

또한, 주요 주요 인터넷 거버넌스 이슈에 대한 교육과 홍보를 통해 보다 많은 시민들이 인터넷 정책결정 과정에 참여할 수 있도록 하고자 합니다. 더불어, 아태 지역 IGF 및 세계 IGF와의 연계를 강화함으로써 한국의 이해당사자들이 지역 및 세계적 차원의 논의에 보다 적극적으로 참여할 수 있도록 하고 있습니다.

한국 인터넷거버넌스포럼은 2012년부터 매해 개최되어 왔으며 2025년에 14회 행사를 개최하게 되었습니다. 2014년부터는 다자간 이해당사자가 참여하는 프로그램위원회를 구성하여 행사를 준비하고 있습니다. 2017년부터 행사에 대한 최종 보고서를 발간하였으며, 세계 IGF에 국가인터넷거버넌스포럼(National IGF)으로 공식 등록되었습니다. 2025년에도 지난해에 이어 최종 보고서를 발간하며, 이를 세계 IGF 사무국에 전달할 예정입니다.

이 보고서에 대한 의견이 있으신 분은 아래 연락처로 의견을 주시기 바랍니다.

o **문의처 :** KrIGF 사무국 (Tel. 02-3446-5934, E-mail. krigf@kiga.or.kr)

1. 2025 제14회 한국인터넷거버넌스포럼(KrIGF) 개요

o 주 제 : ‘인터넷거버넌스의 미래, 우리가 가야할 길’

o 일 시 : 2025년 7월 3일(목), 9:00~18:00

o 장 소 : 세종대학교 광개토관 B1

o 주 최 : 다자간인터넷거버넌스협의회(KIGA)

o 공동주관 : 한국인터넷진흥원, 가비아, 국제메타미디어조합, 나눔비타민, 대전에이블스퀘어, 렛유인에듀, 로켓필름, 페타플래그, 사이버안보연구소, 아시아사회과학연구원, 업폴, 임팩터스, 오픈넷, 정글스튜디오, 정보통신정책연구원, 진보네트워크센터, 카카오, 트루네트웍스, 한국게임이용자협회, 한국인터넷기업협회 (총 20곳)

o 후원 : **과학기술정보통신부(명칭)**, 가비아, 사이버안보연구소, 카카오, 트루네트웍스(총 5곳)

o 홈페이지 : www.krigf.kr

o 참석인원 : **총** 157명 (참석자 121명(77%), Youtube 시청 36명(23%))

* 확인된 이해관계자 구분 총 121명
* 기술계 4명(3%), 산업계 13명(11%), 시민사회 16명(13%), 일반이용자 40명(33%), 공공계 23명(19%), 학계 25명(21%)
* Youtube 참여는 시청한 인원만 카운팅 하였으며, 각 세션마다 중복인원이 있을 수 있음

o 주요결과

- (프로그램) ‘인터넷거버넌스의 미래, 우리가 가야할 길’을 주제로 인공지능, 거버넌스, 디지털 책임 트랙에서 총 9개 워크숍 세션 진행
- 실시간 자막 서비스 제공을 통해 청각장애인의 KrIGF 접근성 보장
- 행사 전후 서포터즈의 적극적인 온라인 홍보, 유튜브 채널 업로드 등을 통한 아카이브 등 한국인터넷거버넌스포럼의 영상 체계화

2. 준비 과정

1) 프로그램위원회

o 한국 인터넷거버넌스포럼은 다자간인터넷거버넌스협의회(KIGA) 산하의 워킹그룹인 한국인터넷거버넌스포럼(KrIGF) 프로그램위원회에서 담당합니다. 현재 프로그램 위원회는 정부, 업계, 학계, 기술계, 시민사회 등 다양한 분야의 참여자들로 구성됩니다.

o 2025년 프로그램위원회는 다음과 같이 구성되었습니다.

- 오경미(위원장), 오픈넷, 시민사회
- 이수영(위원장), 정책과 입법연구소, 시민사회
- 김영규, 인터넷기업협회, 산업계
- 서영진, ICTNet, 시민사회
- 오병일, 진보네트워크센터, 시민사회
- 이 진, 사이버 안보 연구소, 시민사회
- 이종현, 아시아벤처 필란트로피 네트워크(AVPN), 산업계
- 이화영, 사이버 안보 연구소, 시민사회
- 전선민, 정보통신정책연구원(KISDI), 정부
- 전영균, 카카오, 산업계
- 조부승, 한국과학기술정보연구원(KISTI), 기술계
- 조용호, 변혁법제정책연구소, 시민사회
- 최현아, 한국인터넷진흥원(KISA), 정부

2) 프로그램위원회의 준비 과정

o 2025년에 프로그램위원회는 다음과 같이 회의를 통해 행사 준비를 논의하였습니다. 자세한 논의 내용과 회의 결과는 [별첨 1]을 참고하시기 바랍니다

o 1월 24일 : 2025년 프로그램위원회 1차 회의 (제85차 회의)

- 의제(안건) 채택(KrIGF85-1)
- 지난회의록 검토(KrIGF84-2)
- 2025년 KrIGF 프로그램위원회 신청현황 확인
  ▶ 공동위원장 및 NRI 코디네이터 선정
- 2024년 KrIGF 평가 회의록 검토
- 2025년 KrIGF 프로그램위원회 전체일정 검토
- 기타 안건

o 2월 27일 : 2025년 프로그램위원회 2차 회의 (제86차 회의)

- 의제(안건) 채택(KrIGF86-1)
- 지난회의록 검토(KrIGF85-2)
- 2025년 KrIGF 개최장소(안) 공유
- 2025년 KrIGF 트랙 및 논의주제 등 논의
- 2025년 KrIGF 워크숍 세션 모집 일정 및 평가 일정 검토
- 기타 안건

o 3월 27일 : 2025년 프로그램위원회 3차 회의 (제87차 회의)

- 의제(안건) 채택(KrIGF87-1)
- 지난회의록 검토(KrIGF86-2A)
- 포스트 세션 제안서 공유

- WSIS+20 사전 논의 웨비나 준비 현황 공유
- 특정 주요 이슈에 대한 기획 세션의 필요성 검토
- 기타 안건
  - ▸ 장소 관련 변동 사항 공유
  - ▸ 일정 관련(오후·종일)
  - ▸ 서포터즈 모집 기획(안) 공유

o 3월 21일 ~ 4월 30일 : 2025 KrIGF 워크숍 세션 공모 기간

o 4월 7일 ~ 5월 12일 : 2025 KrIGF 서포터즈 모집기간

o 4월 11일 : '국제 디지털 거버넌스 논의 동향과 한국의 대응 방안' 웨비나 개최

o 4월 11일 ~ 5월 30일 : 2025 KrIGF 포스터 세션 공모 기간

o 4월 24일 : 2025년 프로그램위원회 4차 회의 (제88차 회의)
- 의제(안건) 채택(KrIGF88-1)
- 지난회의록 검토(KrIGF87-2)
- 포스트 세션 운영 관련 논의
- WSIS+20 사전 논의 웨비나 결과 공유
- 기타 안건
  - ▸ 장소 관련 변동 사항 공유

o 5월 22일 : 2025년 프로그램위원회 5차 회의 (제89차 회의)
- 의제(안건) 채택(KrIGF89-1)
- 지난회의록 검토(KrIGF88-2)
- 2025 KrIGF 워크숍 세션 모집현황 및 평가 결과 공유
- 2025 KrIGF 전체 프로그램 구성

- 스테이크홀더별 개회사 및 축사 관련 논의
- 2025 KrIGF 슬로건 논의
- 포스트 세션 운영 관련 논의
- 기타 안건
  ▶ 서포터즈 모집 결과 공유
  ▶ 공동주관 및 후원 모집 추천

o 6월 11일 : 2025년 프로그램위원회 6차 회의 (제90차 회의)
- 지난회의록 검토(KrIGF89-2)
- 2025 KrIGF 워크숍 세션 제안서 업데이트 및 패널 현황 확인
- 2025 KrIGF 개회사 및 축사 최종 점검
- 2025 KrIGF 포스터 세션 평가 일정 공유
- 2025 KrIGF 생중계 및 문자 통역 진행 여부 및 예산 확인
- 2025 KrIGF 개최(7.3) 전 행사 점검 회의 필요성 검토

3) 사무국

o 2025년 한국인터넷거버넌스포럼의 준비와 진행을 위해 다음과 같은 분들이 수고해주셨습니다.

- 정길원, KOICS
- 박은하, KOICS
- 김학진, KOICS
- 서　윤, KOICS
- 김정빈, KOICS
- 박해인, KOICS
- 이동근, KOICS
- 이서윤, KOICS
- 이설웅, KOICS
- 이소정, KOICS
- 이효림, KOICS

o (서포터즈)

- 고도원, 경북대학교
- 김도연, 숙명여자대학교
- 김현재, 프리랜서
- 남철우, 연세대학교
- 문필섭, 서울시립대학교 대학원
- 성노아, 홍익대학교
- 엄정우, 성균관대학교
- 이희지, 숙명여자대학교
- 임영조, 단국대학교

- 최연재, 숙명여자대학교
- 허윤영, 한국외국어대학교

4) 페이스북 페이지

o 기존에 페이스북 그룹이 존재하였으나 개인 계정으로 운영이 되었기 때문에, KrIGF의 공식 계정을 통한 조직적인 홍보를 강화하기 위해 2019년 페이스북 페이지를 개설하였음

o 페이스북 페이지 : https://www.facebook.com/krigf.kr/

5) 유튜브 채널 개설 및 KrIGF 동영상의 체계적인 관리

o 과거에 촬영되었던 영상을 포함하여 유튜브 채널을 통해 체계적으로 관리하기로 함

o 유튜브 채널 : https://www.youtube.com/@2025KrIGF

6) 문자통역

o 장애인 접근성 보장 및 속기록을 남기는 의미에서, 문자통역을 제공하기로 함.

o 사회적 협동조합 에이유디 실시간 문자통역 서비스 이용.

3. 프로그램

트랙1	트랙2	트랙3
인공지능	거버넌스	디지털 책임

시간	내용		
13:00 ~13:30	**개회식** □ **사 회 : 오경미**(KrIGF 공동위원장) □ **인사말 :** 이동만(KIGA 위원장) □ **축 사 :** 박지현(과학기술정보통신부 과장) **(영상)**이해민(조국혁신당 국회의원)		□ **개회사** - 공 공 계 : 이동근(KISA, 본부장) 또는 박정섭(KISA, 센터장) - 시민사회 : 오병일(진보네트워크센터, 대표) - 기 술 계 : 김진수(KISIA, 수석부회장) - 학 계 : 이동만(KIGA, 위원장) - 산 업 계 : 박성호(한국인터넷기업협회, 회장) 김영규 정책실장 대독
13:40 ~15:00 (80')	**지브리 스타일 생성형 AI 이미지 열풍이 던진 질문** ■ 사회 : 이수영(정책과 입법연구소) ■ 발제 : 정일진(17정글 스튜디오) ■ 토론 : 조용호(변혁법제정책연구소) 전영균(카카오) 조윤재(신한대학교) 김나영(루트소리연구소) 이창범(연세대학교)	**등록 제한 도메인이름(유보어) 개방 정책 논의** ■ 사회 : 강경란(아주대) ■ 발제 : 이정민(KISA) ■ 토론 : 오병일(진보네트워크센터) 이명수(메가존) 이예진(이화여대)	**혁신과 책임의 경계에 선 디지털 트윈 기술의 두 얼굴과 미래** ■ 사회 : 배정철(동의대) ■ 발제 : 이예림(업폴) ■ 토론 : 염세경(동국대) 민재명(한국열린사이버대) 이진(사이버안보연구소) 윤성열(사이버안보정책청년연구회)
15:00~ 15:10	**휴식**		
15:10 ~16:30 (80')	**AI 윤리 레터 : 성과 보고를 통해 살펴보는 한국 AI 윤리 대중 담론의 현재와 미래** ■ 발제 : 고아침(AI 윤리 레터) ■ 토론 : 권오현(사회적협동조합빠띠) 송수연(언메이크랩)	**인터넷 기업의 상생 및 ESG 방향성** ■ 사회 : 전영균(카카오) ■ 발제 : 권현옥(카카오) ■ 토론 : 오경미(오픈넷) 이정민(KISA) 전선민(KISDI) 성정모(광운대학교 4학년)	**AI 기반 보이스피싱의 진화와 디지털 신뢰 체계의 위협** ■ 사회 : 김민지(숙대) ■ 발제 : 이지현(숙대) ■ 토론 : 정용욱(서울청 사이버수사과) 강대규(금융보안원) 정수민(숙대) 최다연(숙대)
16:30~ 16:40	**휴식**		
16:40 ~18:00 (80')	**인권과 평화를 위협하는 군사 인공지능, 이대로 괜찮은가** ■ 사회 : 고아침(AI 윤리레터) ■ 토론 : 김윤명(디지털정책연구소) 이화영(사이버안보연구소) 뎡야핑(팔레스타인평화연대) 박해룡(KISA) 김한민영(국제엠네스티 한국) 최효민(서울대학교 박사과정) 케이트 심(Tech Workers Coalition)	**WSIS+20와 향후 국내외 글로벌 인터넷거버넌스 논의 대응 방향** ■ 사회 : 박민정(KISDI) ■ 발제 : 전선민(KISDI) ■ 토론 : 전영균(카카오) 오병일(진보네트워크센터) 송혜인(KISA) 양지수(이화사회과학원) 정다현(이화여대)	**불안의 시대, 당신의 정보는 안녕하십니까? - SKT 유심 정보 유출 사고와 존재론적 안보** ■ 사회 : 민병원(이화여대 교수) ■ 발제 : 강세은, 김기영, 김하은, 도가영, 임규리 (이화여대) ■ 토론 : 심동욱(KISA) 이진규(네이버) 김현이(법무법인 세종) 최홍규(EBS)

o 세부적인 워크숍 세션 논의 결과는 [7. **워크숍 세션 세부내용**]을 참고하시길 바랍니다.

4. 행사 평가

1) 참석자 통계

o 총 사전등록자 : 185명 / 설문조사 응답 인원 : 78명

o 참석인원 : **총** 157명 (사전등록 참석자 81명(53%), 현장등록자 40명(25%), Youtube 참여 약 36명(22%))

* 확인된 이해관계자 구분 총 121명
* 기술계 4명(3%), 산업계 13명(11%), 시민사회 16명(13%), 일반이용자 40명(33%), 공공계 23명(19%), 학계 25명(21%)
* Youtube 참여는 시청한 인원만 카운팅 하였으며, 각 세션마다 중복인원이 있을 수 있음

2) 만족도 조사결과

1. 설문 참여자 분포 (총 78명 응답)	공공계(14)	학계(17)	산업계(10)	시민사회(7)	기술계(3)	이용자(27)
	18%	22%	13%	9%	4%	34%

2. 한국인터넷거버넌스포럼 참여 경험	**있음(42명)**	54%
	없음(36명)	46%

3. 워크숍 세션 만족도 (오후1 세션)	**워크숍**	**내용 유익성**	**시간 적절성**
	세션1 : 지브리 AI (36명 응답)	92%	87%
	세션2 : 유보어 개방정책 논의 (19명)	95%	88%
	세션3 : 디지털 트윈 (19명 응답)	90%	90%

4. 워크숍 세션 만족도 (오후2 세션)	**세션4 : AI 윤리 레터 (22명 응답)**	93%	92%
	세션5 : 인터넷 기업 상생 (25명 응답)	92%	91%
	세션6 : AI 기반 보이스 피싱 (27명 응답)	92%	89%

5. 워크숍 세션 만족도 (오후3 세션)	**세션7 : 군사 인공지능 (22명 응답)**	89%	90%
	세션8 : WSIS+20 (23명 응답)	94%	89%
	세션9 : 유심 정보 유출 (29명 응답)	91%	90%
6. 행사장 만족도	**행사장 시설 (78명 응답)**	88%	

7. 기타 의견	- (시민사회) 세션5를 참여하고 기업 ESG 활동과 인터넷 접근성 증진 노력에 대해 새롭게 알게 되어 의미 있는 경험이었습니다. - (학계) 세션6을 참여하였는데, 현실적인 피해와 정책적 대안이 함께 제시되어 유익했습니다. - (공공) 행사장 동선은 조금 불편했으나 안내 등은 잘 되어있었음. - (산업계) 세션별 주제와 다룰 내용, 패널 정보 등을 간단히 정리한 자료집을 사전에 배포했으면 합니다. - (학계) 행사가 끝나고 유튜브에 자료와 영상이 제공되어 다시 한 번 볼 수 있어서 좋았습니다. - (이용자) 세션9에 참여했는데, 패널 구성이 다양하고 전문성을 갖추고 있어서 정보의 유익성과 토론의 완성도 면에서 높은 만족도를 느꼈습니다. - (기술계) 세션9는 AI를 기반으로 한 보이스피싱이라는 주제가 신선했고 유익했습니다. - (학계) AI 기술이 잘못 사용될 경우, 발생할 수 있는 리스크를 다시 인식할 수 있었습니다.
8. 내년 희망하는 KrIGF 논의주제 및 논의 장소	- 주제 : AI 관련 ▸ AI로부터 개인정보보호, AI 윤리, AI 거버넌스 - 주제 : 디지털 신뢰 및 보안 관련 ▸ RDAP/RPKI, 메타버스 정보보안, 초국가적 사이버안보, S/W 임베디드 보안 - 주제 : 거버넌스 ▸ 디지털 청년세대의 알고리즘 피로, 디지털 격차, 기업 ESG 활동 - 희망 장소 ▸ 수도권 내 호텔, 전문 전시홀, 상명대학교, 세종대학교, 프란치스코 교육회관, 천안 또는 대전에서 개최하면 어떨지? ▸ 실내 공기를 환기할 수 있는 쾌적한 환경이었으면 함. 세종대의 경우 공기가 답답하고 더움.

3) 프로그램위원회 자체 평가

o 2025 KrIGF 프로그램위원회 자체 평가 및 개선방안 논의

- (오병일) 포스터 세션은 공간 및 시간적인 제약으로 인해 별도의 공간이 필요할 것 같음. 참석자 수가 전년 대비 40~50명 정도 줄었는데 오전 세션을 운영하지 않아서인지 홍보가 부족했기 때문인지 분석이 필요함. 다만 오후 진행으로 참석자 수가 끝까지 유지된 점은 긍정적임.
- (전선민) 포스터 세션은 모든 제안자가 같은 시간에 심사받을 수 있도록 하되 전시·배치 개선도 고민할 필요가 있음. 장소 접근성 문제로 참석자가 줄었을 수도 있으며, 오후만 진행하여 효율적으로 운영할 수 있었음.
- (전영균) 개인적으로 올해 KrIGF가 가장 좋았고 오후만 운영한 덕분에 참석자들이 끝까지 남아있었고 집중도도 높았음. 포스터 세션 또한 의미가 있었음. 행사장 환경이 다소 답답했다는 점에 공감하고 내년에는 환경에 대한 고려가 필요하다고 생각함.
- (조부승) 최근 해외 학술 포럼을 참여했고, 해외에서는 기술적인 주제가 활발히 다뤄짐. 특히 연구망·보안 관련 글로벌 협력 논의를 KrIGF 세션에 반영하면 국제 연계성과 전문성을 높일 수 있을 것임.
- (이화영) 포스터 세션은 학생들이 참여할 수 있는 새로운 기회가 되었으나, 운영 방식을 조금 더 체계화할 필요가 있음.
- (김영규) 반나절 집중하여 운영하니 종일보다는 임팩트 있고 효율적인 것 같았음. 예상보다 참석자 수가 많아 긍정적으로 느꼈고, 작년과 재작년의 경우는 Youth를 위한 트랙이 많았던 것 같은데 올해는 다소 줄어든 것 같음.

o 정리

- 오후 집중 운영에 대해 대부분 위원이 긍정적인 평가
- 포스터 세션 체계화 및 운영 방식 개선 필요
- 참석자 수 감소에 대한 홍보·장소 접근성 개선 필요

5. 결산

제14회 한국인터넷거버넌스포럼(KrIGF) 세부지출 내역

'25.08.21(목), 다자간인터넷거버넌스협의회(KIGA) 사무국

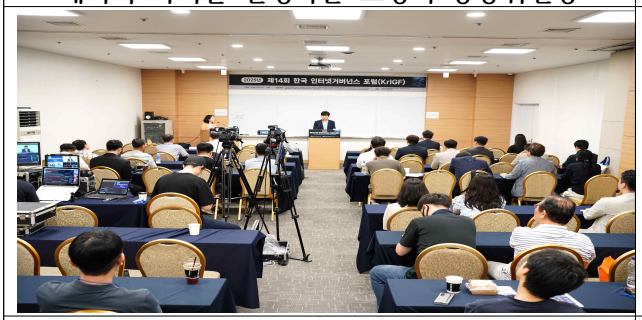
항목	세부항목	수량	단가(원)	예산(원)	비고
행사장 임대료	행사장/사무국대기실 등	4실	-	2,222,000	
전문가활용비/인건비	세션별 문자통역비	1식	-	2,271,500	
	서포터즈 지원비	11명	100,000	1,608,000	우수서포터즈(3)/포스터 상금(4) 포함
	현장 지원인력	7명	100,000	743,500	
	영문 번역비	1식	-	1,000,000	예정
온라인생중계/장비임차	유튜브/줌 생중계운영	1식	-	7,050,000	사진촬영 포함
	노트북 대여	8대	50,000	400,000	
	유선인터넷 설치	4회선	50,000	200,000	
기념품/기프트카드, 식대 및 다과, 음료 등	기념품/기프트카드	1식		2,880,000	VIP 기념품 포함
	참가자 다과, 음료, 정수기, 주차지원 등	1식	-	4,279,930	프로그램위원 저녁포함
홍보 및 홍보물 제작	홍보/웹자보/현수막/배너/포스터 제작 등	1식	-	3,713,050	
인쇄 및 사무용품 등	인쇄, 문구류, 명패, 명찰, 토너 등	1식	-	1,896,510	
총 지출금액				**28,264,490**	

※후원 현황: 카카오(250만원), 가비아(100만원) 후원 350만원

- 사업비: 25,000,000원(예산) + 3,500,000원(후원금) = 28,500,000원

6. KrIGF 행사 사진

1) 개회식

<table>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>개회식 사회를 진행하는 오경미 공동위원장</td><td>개회사를 연설하는 KIGA 이동만 위원장</td></tr>
<tr><td>  </td><td> 
</td></tr>
<tr><td>공공계를 대표하여 연설하는 KISA 박정섭 단장</td><td>2025 KrIGF 개회식 단체사진</td></tr>
</table>

2) 트랙1

<table>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>지브리 스타일 생성형 AI 이미지 세션</td><td>AI 윤리 레터 세션</td></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>인권과 평화를 위협하는 군사 인공지능 세션</td><td>포스터 세션 시상 단체 사진</td></tr>
</table>

3) 트랙2

<table>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>등록 제한 도메인이름 개방 정책 논의 세션</td><td>인터넷 기업의 상생 및 ESG 세션</td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>WSIS+20 세션</td><td>세션 질의응답</td></tr>
</table>

4) 트랙3

<table>
<tr><td>  </td><td> 
</td></tr>
<tr><td>디지털 트윈 기술의 두 얼굴과 미래 세션</td><td>AI 기반 보이스피싱 세션</td></tr>
<tr><td> 
</td><td>  </td></tr>
<tr><td>유심 정보 유출 사고와 존재론적 안보 세션</td><td>세션 질의응답</td></tr>
</table>

7. 워크숍 세션별 결과보고서

2025 한국인터넷거버넌스포럼(KrIGF) 워크숍 세션 보고서

작성자 : 이수영

세션명	지브리 스타일 생성형 AI 이미지 열풍이 던진 질문			
일시	2025. 7. 10. (목), 13:40~15:00		장소	세종대학교 광개토관(1+2호)
참석자	사회	이수영(정책과입법연구소의장)	발제	정일진(정글17 스튜디오 대표)
	패널	전영균(카카오 사회협력 수석)		조윤재(신한대학교 교수)
		김나영(루트소리연구소 대표)		이창범(연세대학교 법무대학원 교수)

제안내용	◎ 제안 취지 및 주요쟁점 디지털 기술의 발전은 문화예술 분야에서 새로운 변화를 불러일으키고 있다. 전통적인 문화예술 형식이 디지털 매체와 결합하면서 새로운 형태의 예술이 확산되고 있다. 문화예술의 창작자들은 AI를 비롯한 디지털 신기술을 적극적으로 활용해 새로운 창작 방식을 만들어내면서 문화예술의 경계를 확장하고 있다. 또한, 이러한 변화는 예술 창작 방식 뿐만 아니라, 문화예술에 대한 소비 및 유통 등 다양한 측면에 영향을 주고 있다. 이에 인공지능 등 디지털 기술을 활용한 예술 창작 사례를 소개하고, 디지털 기술이 예술가의 창작 과정에 미치는 긍정적, 부정적 영향을 함께 살펴볼 것이다. 특히, AI가 생성한 작품이 진정한 예술로 인정받을 수 있는지, AI가 예술가의 창작물에 미치는 영향은 무엇인지 살펴볼 것이다. 또한, Instagram, YouTube, 그리고 다양한 스트리밍 서비스를 중심으로 한 문화예술의 유통 방식의 변화가 예술가와 시장, 관객 간의 관계를 어떻게 설정하는지 다룰 것이다. 또한, AI 기술이 발달하면서 모방과 창조의 경계가 점점 흐려짐에 따른 법적, 윤리적, 사회적 문제와 쟁점을 짚어볼 것이다. 예컨대, AI 등 디지털 기술의 발전이 문화예술 창작자를 대체할 것인지, 그로 인해 예술가를 위한 일자리가 줄어들어 생계에 부정적 영향을 줄 것인지, 아니면 더 큰 기회를 제공할 것인지 살펴볼 것이다. 나아가, AI가 생성한 음악이나 그림 등 문화예술에 대한 저작권이 누구에게 귀속되는지, 부정경쟁방지법이 적용가능한지, AI가 생성한 작품에 대한 법적, 윤리적 책임은 누구에게 있는지, NFT 디지털 아트의 재판매 보상청구권 등에 대해 함께 검토할 것이다. 이 세션은 디기술이 문화예술 창작 및 유통 방식에 미치는 영향을 다각도로 분석하고, AI와 관련된 법적 및 윤리적 쟁점을 심도 있게 논의하는 자리가 될 것이다. 참가자들은 이러한 변화가 예술가와 관객, 그리고 시장에 미치는 영향을 이해하고, 앞으로의 방향성을 모색하는 기회를 가질 것이다. 사회자 이수영, 정책과 입법연구소 의장, 시민사회 발제자 정일진, 17정글 스튜디오 대표, 기술계 토론자 이창범, 연세대학교 법무대학원 겸임교수, 학계 전영균, 카카오 사회협력 수석, 산업계

	조윤재, 신한대학교 교수, 학계 김나영, 루트소리연구소 대표, 문화예술 창작자, 청년 * 패널의 의견은 그 단체 또는 소속의 의견이 아님을 알려드립니다.
요약내용	**사회자 : 이수영** (정책과입법연구소의장/KrIGF 위원장) • 오늘의 주제는 '지브리풍 AI 이미지' 열풍이 예술, 사회, 법에 어떤 질문을 던졌는지 탐색하는 것. • 생성형 AI 는 창작 방식, 유통 구조, 소비 방식까지 문화예술계 전반을 뒤흔들고 있음. • 다양한 전문가들과 함께, 예술성과 창작자 권리, 기술의 사회적 책임, 법적 과제 등을 논의함. **발제 : 정일진 대표 (정글 17 스튜디오 대표)** "단순한 놀이 같지만, 윤리적 고민이 필요한 사회 현상입니다." **1. 현상 설명** ○ 2025 년 3 월, 카카오톡 프로필을 중심으로 '지브리풍' AI 이미지 생성 붐이 일어남. ○ 대부분의 국민이 자기 사진을 업로드하고, AI 가 생성한 일러스트를 저장 및 공유. ○ 부모 세대까지 확산될 정도로 사회 전반적 유행을 이룸. **2. 세 가지 핵심 쟁점 제기** ○ **① 얼굴 데이터 제공의 무의식성** → 대중은 개인정보 제공의 위험성을 인지하지 못한 채 얼굴 이미지를 업로드. → AI 학습과 활용에 자기 얼굴이 사용될 수 있다는 점에서 개인정보 이슈 발생. ○ **② 에너지 소비 문제** → 이미지 한 장 생성에 들어가는 GPU 사용량은 스마트폰 수십 대 충전 수준의 전력 소모. → "놀이" 수준의 AI 이미지가 대규모 전력 낭비로 이어지는 구조. ○ **③ 창작 윤리 vs 편리성** → 미야자키 하야오 감독이 수년간 그려온 창작물의 가치를 AI 가 "딸깍 한 번"에 복제. → 창작에 대한 존중 없이, 비주얼만 소비하는 '편의주의적 예술 소비'의 위험성 제기. **패널 토론 요약** 1) **1. 전영균 수석 (카카오 사회협력실)** "AI 는 도구일 뿐, 핵심은 그것을 활용하는 인간의 창의성과 태도에 달려 있다."

- AI 는 연필, 포토샵처럼 **창작 도구 중 하나**일 뿐.
- 그러나 콘텐츠 소비자와 제작자 모두 **'AI 개입 여부'를 인식할 권리**가 있음.
- 카카오는 AI 콘텐츠에 **워터마크·태깅 등 투명성 확보 방안**을 내부적으로 논의 중.
- 법적 규제 이전에, **플랫폼 차원의 책임 있는 디자인**이 필요하다고 강조.

2. 조윤재 교수 (신한대학교 교수) "기술의 윤리적, 환경적 비용에 무감한 AI 사용은 디스토피아로 이어질 수 있다."

- 지브리풍 AI 이미지 유행은 **소비주의적 테크 사용의 전형적인 사례**로 봐야 함.
- GPU 수요 폭증, AI 연산으로 인한 탄소배출 증가 등 **환경적 책임**을 간과 중.
- 오픈 AI 의 CEO 샘 알트만의 말처럼, "GPU 가 모든 걸 결정짓는 시대"가 되고 있음.
- AI 이용의 **사회적 비용과 생태적 대가**에 대한 교육과 정책적 고민 필요.
- 특히, AI 활용이 **실질적인 창작인지, 단순 모방 소비인지** 구분 필요.

3. 김나영 대표 (루트소리 연구소, 전통예술가) "AI 는 창작을 죽이지 않는다. 오히려 창작자에게 시간을 돌려준다."

- 전통예술가 입장에서, AI 는 **보완재 혹은 '창작 보조 장치'로 유용**함.
- 예: 전통음악을 AI 로 시각화하거나, 영상 콘텐츠에 빠르게 적용 가능.
- 현재 한국의 저작권 체계는 "AI 가 일부라도 개입한 작품은 저작권 등록 불가" → 이는 지나치게 폐쇄적이며, 창작의 미래를 막는 제도.
- 미국의 사례처럼, **AI 개입 + 인간의 의도적 편집이 있으면 저작권 인정해야 함**.
- 결론: 예술계는 AI 를 경계할 것이 아니라, **적극적으로 길들이고 활용해야 함.**

4. 이창범 교수 (연세대 법무대학원) "AI 학습 자체는 위법 아님. 침해는 '결과물 유사성'에 달려 있다."

- 현재 법 체계 상, **AI 가 책·이미지를 학습하는 것 자체는 저작권 침해로 보기 어려움**
  (사람이 책을 읽고 그림을 그리는 것과 동일하게 간주)
- 저작권 침해 판단 기준은 **"결과물이 실질적으로 기존 창작물과 유사한가"**
- AI 개발자에게 광범위한 책임을 묻기보다는, **사용자 책임과 윤리 규범 정착이 우선.**
- 법적 규제만으로는 한계가 있어, **소프트 로(law)** 차원의 사회적 합의 중요.

논의 세부 내용

구분	주요 내용
예술성	AI 는 도구일 뿐, 창작 의도와 인간의 기획이 본질이라는 관점 다수
저작권	AI 학습 자체는 저작권 침해가 아님. 그러나 결과물 유사성 논란 존재.
책임 구조	창작자, AI 개발자, 플랫폼 간 책임 분배가 불명확하므로 제도 정비 필요
투명성 확보	생성 콘텐츠에 AI 개입 여부 표시 필요 (워터마크 등)

구분	주요 내용
환경 문제	AI 이미지 생성 시 탄소 배출량 문제 제기 → 윤리적 사용 필요
직업과 창작	예술가는 AI 를 통해 생산성 향상, 창작 집중 가능하나, 권리 보호 필요

주제	쟁점 요약	패널 의견
예술성과 창작	AI 는 창작 도구일 뿐, 예술성은 인간의 기획과 편집에 달려 있음	대부분 동의. 단순 복제 소비 문화는 경계해야 함
개인정보 / 얼굴 이미지	얼굴 데이터를 무의식적으로 제공하는 구조 문제	사용자 인식 개선 및 플랫폼의 책임 필요
저작권 문제	AI 학습 자체는 침해 아님. 결과물 유사 여부가 핵심	한국은 지나치게 보수적. 미국 사례처럼 유연성 필요
환경 비용	AI 사용 시 전력 소모 및 탄소배출 등 생태적 문제 발생	기술 사용에 대한 윤리적 교육 및 정책 필요
제도 및 법률	법보다는 사회적 윤리 기준, 플랫폼 책임, 사용자 자정이 중요	'하드 로'보다는 '소프트 로' 중심 대응 필요
창작자 직업 안정성	AI 가 예술가 일자리를 대체할 것인가?	오히려 창작자에게 시간과 자율성을 부여할 수 있음

워크숍 총평

2025 년 7 월 10 일 제 11 회 한국인터넷거버넌스포럼(KrIGF)에서 열린「지브리 스타일 생성형 AI 이미지 열풍이 던진 질문」세션은, 최근 대중적으로 확산된 AI 이미지 생성 열풍을 계기로 기술과 사회, 예술, 법, 환경 등의 쟁점을 입체적으로 조명한 의미 있는 자리였음.

1. **생활 밀착형 주제로 공감도 높은 문제의식 제기**
   - 지브리풍 이미지 열풍이라는 **현실적인 사회문화 현상**을 다뤄, AI 기술에 생소한 일반 시민도 주제에 쉽게 접근할 수 있었음
   - 예: "부모님까지 프로필 사진을 AI 이미지로 바꾼 현상"이라는 도입 설명은 현장의 몰입도를 높이는 데 효과적이었음
2. **다양한 분야의 전문가 참여로 다각적 논의 가능**
   - 법학자, 예술가, 플랫폼 기업, 정책학자 등 **서로 다른 시각의 패널 구성**으로 토론의 깊이와 균형을 확보함.
   - 특히 루트소리연구소 김나영 대표의 "AI 는 창작자를 위협하는 것이 아니라 시간을 돌려주는 도구"라는 발언은, 예술계 안에서도 다양한 스펙트럼이 있음을 보여주며 참여자들의 반응이 좋았음.
3. **'기술 유행'에서 '사회적 성찰'로 확장한 구성**
   - 단순히 '지브리 이미지가 귀엽다/무섭다'는 차원을 넘어, **AI 이미지 소비가 가지는 윤리적, 생태적, 제도적 문제**까지 폭넓게 조망함.
   - 조윤재 교수의 "GPU 가 모든 걸 결정하는 시대"라는 언급은 기술 소비의 환경적 비용을 일깨워준 인상적인 사례였음.
4. **실천적 대안 언급이 포함됨**
   - 카카오 전영균 수석이 언급한 "AI 콘텐츠에 워터마크·태깅을 붙이는 방식" 등 **플랫폼 차원의 투명성 확보 방안** 제안은 실질적인 후속 논의의 단초가 됨.

🕐 **미디어·청소년 관점 부족**

	• 생성형 이미지 콘텐츠는 청소년, 유튜브, SNS 등 **디지털 네이티브 세대**의 활용이 가장 활발한데, 해당 세대의 윤리 교육, 미디어 리터러시 문제 등은 **상대적으로 소외**되었음. • 향후에는 **10 대·20 대 이용자 경험, 미디어 교육 전문가 의견** 등을 포함해 균형 잡힌 시각 제공 필요. 🕐 **환경 문제 논의가 구조적 해결 방안 없이 종료** • GPU·전력소비·탄소배출에 대한 문제 제기는 인상 깊었지만, → 구체적인 해결책(예: AI 연산 최적화, 탄소세, 윤리적 GPU 사용 가이드라인 등)이 논의되지 않아 **문제 제기 수준에서 멈춤**.

2025 한국인터넷거버넌스포럼(KrIGF) 워크숍 세션 보고서

작성자 : 황해란

세션명	등록 제한 도메인이름(유보어) 개방 정책 논의			
일시	2025. 7. 3. (목), 13:40~15:00		장소	세종대학교 광개토관 B1
참석자	사회	강경란(아주대학교 교수)	발제	이정민(한국인터넷진흥원 팀장)
	패널	이정민(한국인터넷진흥원 팀장)		이예진(이화여자대학교 학생)
		오병일(진보네트워크센터 대표)		
		이명수(메가존 차장)		

제안내용	○ 제안 배경 - 제7차 인터넷주소자원 기본계획('24~'26)에 의거하여 등록 제한 도메인이름(유보어) 개방 검토 필요성 논의 진행. - 유보어 정책 방향은 지정 취지, 근거에 대한 유효성 여부를 확인해야 하며, 개방 이후 돌이킬 수 없으므로 신중한 검토 필요. - 한국인터넷진흥원이 국내 인터넷 이용자를 대상으로 실시한 '유보어 개방에 대한 설문조사*' 결과, 유보어 개방에 대해 국가·행정구역명 유보어는 69.5%, 일반명사 유보어는 75.6%, 성씨 영문표기 유보어는 69.8%의 응답자가 긍정적으로(타당+매우타당) 응답하였으며, 비속어/비윤리 유보어는 29.6%만이 응답자가 긍정적으로 응답. * 시기 및 응답자: 2025. 3. 14. ~ 23. (894명 응답) ○ 제안 취지 - 도메인이름의 안정적 관리, 공공의 이익을 위해 등록을 제한하는 도메인이름(유보어)의 개방 필요성 및 대상·방식·유보어의 선정과 관련하여 다양한 이해관계자들의 의견이 반영될 수 있도록 의견을 청취하고자 함.
요약내용	○ 유보어 소개 - (정의) 도메인이름 사용에 있어서 향후 사용이 예상되는 이름의 보호 - (배경) 공공의 이익과 안정적 운영, 사회적 책임 및 윤리적 기준 준수를 위해 도입 - (현황) 7,282개로, 종류는 일반명사, 지역명, 비속어, 한 글자, 공공기관 관련 등 다양 - (개방 필요성) 시대 변화와 '한글.kr' 도메인 등록(4.6만 건)에 따라 활성화 유도 필요 특히, '한글.kr'은 타 도메인 대비 등록 제한이 많음 - (설문조사 결과) 국민의 75.6%가 일반명사 유보어 개방에 찬성 ○ 유보어 개방 정책 초안 - (대상) '한글.kr'의 일반명사 유보어(753개) - (방식) 선접수·선등록 - (시기) 2025년 내 개방

논의 세부 내용	○ 이정민 팀장 - '유보어'란 혼란 방지, 공공성 보호, 도메인 공간의 잠재적 활용 가능성 등을 고려하여 등록이 제한된 도메인으로, 총 7,282개가 존재. 유형은 일반명사, 지역명, 비속어, 한 글자, 공공단어 등으로 나뉘며, 특히 '한글.kr' 도메인의 일반명사(예: 병원, 꽃집 등)는 753개가 유보된 상태. 이는 향후 3단계 kr도메인 확장 운영을 고려한 선제적 조치였으나, 현재까지 유보어를 사용한 3단계 도입이 이루어지지 않았고 등록률도 저조해 개방 필요성이 커짐. 이러한 상황을 종합해 보면 유보어 개방이 시대적 흐름에 부합하며, 현재 .com, .net 등 타 도메인에서는 동일한 단어가 이미 등록되어 있어 형평성 문제가 존재함. 대국민 설문조사에서는 전체 응답자 중 75.6%가 일반명사 유보어 개방에 찬성함을 확인하였고, 이에 한국인터넷진흥원은 일반명사 개방을 중심으로 개방 정책 초안을 마련했으며, '선접수·선등록' 방식을 제안 함. 다만 사이버스쿼팅 우려와 공공 단어의 사익 활용에 대한 문제점도 고려하고, 개방 범위(예: 비속어, 지역명 등)와 방식(조건부 등록, 추첨, 경매 등)에 대한 다양한 의견 수렴을 위해 본 공청회를 마련했다고 밝힘. ○ 오병일 대표 - 유보어 개방에 대해 원칙적으로 찬성하며, 특히 유보어 유지의 정당성에 대한 재검토가 필요함을 강조. 현재 유보어로 지정된 단어들이 어떤 근거와 맥락에서 지정되었는지에 대한 당시 기록이 부족하며, 정책의 신뢰성과 일관성을 위해 유형별 목적 및 기준을 명확히 해야 한다는 입장. 비속어 유보어에 대해서는 비판적 시각을 제시했는데, 예를 들어 '미친놈'과 같은 단어는 맥락에 따라 중립적·긍정적 의미로도 활용될 수 있으므로(예: 공부에 미친놈) 도메인 등록을 일괄 제한하는 것은 과도함. 또한, 지역명 유보어 관련해서도 특정 지자체에 우선권을 부여하는 것은 타당하지 않으며, 일반 이용자나 기업이 활용함으로써 지역 경제 활성화에 기여할 가능성도 있음. 개방 방식에 대해서는 '선접수·선등록'이 가장 현실적이고, 해당 방식이 일반적인 도메인 정책 흐름에 부합함. 사이버스쿼팅 우려는 기존 도메인에서도 존재하는 문제로, 별도의 정책을 둘 이유가 부족함. 유보어 외에도 예약어의 개념이 불분명한 점, 도메인별 정책 간 불일치 문제를 짚으며 정책 정비의 필요성을 제기. ○ 이명수 차장 - 국가도메인 등록대행자인 메가존의 실무자이자 시장 참여자로서 유보어 개방에 찬성 입장이나, 개방 방식과 절차에 대한 체계적 준비가 필요함. 기존 도메인이름과 동일한 키워드의 유보어가 개방될 경우 이용자가 혼란을 겪거나, 기존 도메인 등록인들이 의도치 않은 손해를 볼 수 있다고 지적하며, 기존 등록인(예: 꽃집.한국)에게 사전 안내를 통해 신속히 등록할 수 있는 기회를 제공하는 방안을 고려할 것을 제안. 또한, 유보어 개방 시 기업이나 개인이 등록 기회를 놓치지 않도록 충분한 홍보가 이루어져야 하며, 이의제기 절차 및 분쟁 해결 방안도 함께 마련되어야 함. 이전 유보어 정책이 3단계 도입 가능성을 전제했으나, 현재는 도메인 사용 환경이 변화했으며, 동일한 일반명사가 타 도메인(TLD)에서 이미 널리 사용 중인 상황에서 '.kr'만 제한을 두는 것은 시장 경쟁력 측면에서도 바람직하지 않음. 즉, 개방은 찬성하되, 관련 이해당사자들의 권리 보호를 위한 절차적 보완이 필요하다는 현실적 접근을 제안.

	○ 이예진 학생 - 청년 세대이자 일반 인터넷 이용자의 시각에서 유보어 개방에 대한 의견 제시. 개방에는 찬성하면서도, 이용자가 인지하는 도메인의 실제 활용 방식에 비추어 볼 때, '.한국'과 '.kr'이 최상위 도메인만 다를 뿐 실질적으로 같은 주소로 오인될 수 있는 가능성이 크다고 지적. 이로 인해 이용자는 혼동하거나 잘못된 사이트에 접속할 우려가 있으며, 이는 신뢰도 저하로 이어질 수 있다는 점에서, 유보어 개방 시 사전 홍보와 안내는 반드시 병행되어야 함. 또한, '.한국' 도메인을 이미 보유한 등록인에게는 '.kr' 도메인 등록 시 우선권이나 사전고지 기회를 부여하는 방안이 이용자 권익 측면에서 고려될 수 있음. 개방 자체를 막을 수는 없으나, 도메인의 특성상 일반 이용자가 직접 활용하거나 접속하는 경우가 많으므로, 혼란을 줄이기 위한 정책이 중요함. 개방이 '인터넷의 평등성과 개방성'이라는 원칙에 부합하기 위해서는 충분한 이용자 배려가 전제되어야 함. ○ 윤복남 변호사(일반 참석자) - 이번 유보어 개방 논의가 특정 사례에 국한되지 않고 전체 국가도메인 정책의 일관성과 체계성을 점검하는 계기가 되어야 함. 현재 유보어 정책이 도입 시기와 목적에 따라 제각기 설정되어 있어, 유형 간 기준이 명확하지 않으며, '.kr', '.한국' 도메인 간에도 동일 단어의 사용 가능 여부가 달라 정책 혼선이 발생할 수 있음. 예컨대 한글 한 글자 유보어의 경우, '.kr'에서는 2,000개 이상이 유보 상태이나, '.한국'에서는 이미 개방되어 있음. 유보어 개방을 일반명사부터 시작하는 것에 동의하며, 이후 지역명, 한 글자, 공공기관 관련 유보어 등도 차례로 논의하는 중장기 로드맵도 필요. 또한, 등록 방식은 실용성과 공정성을 고려할 때 '선접수·선등록' 방식이 가장 현실적이라 판단했으며, 이로 인한 과열이나 오용 우려는 기존의 분쟁조정제도 등을 통해 충분히 조정 가능함. 더불어 상표권 보호를 위한 보완 제도를 마련하는 것도 함께 논의되어야 할 사안으로 제안.
워크숍 총평	개방에 대해 전반적으로 찬성하면서도 개방 방식과 우선권 부여 여부에 대해 다양한 의견이 있었음. 오병일 대표는 "굳이 막을 이유가 없다"는 관점에서 유보어 유형별 존치 근거 재정비와 전면 개방을 주장했고, 이명수 차장은 기존 이용자 혼란 방지를 위한 기존 등록인 대상 우선권 제공이나 사전고지 필요성을 강조했고, 이예진 학생 역시 이용자 측면에서 도메인 간 혼동 우려를 제기하며 "등록인 보호와 홍보가 병행되어야 한다"는 입장. 플로어의 일반 참석자인 윤복남 변호사는 유보어 개방을 넘어 각 도메인 정책 간의 일관성 확보를 당부. 사회자인 강경란 교수는 "개방 여부가 아닌 '어떻게 개방할 것인가'가 핵심"이라고 짚으며, 유보어 대부분이 20년 전 지정된 것임을 언급하며, "세대 간 언어 사용과 사회적 인식이 바뀐 만큼 변화에 대한 정책적 대응도 필요하다"고 언급. 현장 참여자들의 투표 결과를 통해서 개방에 대한 공감대가 형성되었음을 확인했으며, 비속어, 한 글자, 지역명 등 일부 민감한 유형의 유보어에 대해서는 여전히 신중한 접근이 요구된다는 점도 드러남. 이번 공청회는 유보어 개방에 대한 사회적 합의 형성의 출발점이자, 향후 정책 설계 시 공공성과 실용성, 형평성 간 균형을 고민해야 할 필요성을 환기한 자리가 되었음.

2025 한국인터넷거버넌스포럼(KrIGF) 워크숍 세션 보고서

작성자 : 이예림

<table>
<tr><td>세션명</td><td colspan="4">혁신과 책임의 경계에 선 디지털 트윈 기술의 두 얼굴과 미래</td></tr>
<tr><td>일시</td><td colspan="2">2025. 7. 3. (목), 09:00~18:00</td><td>장소</td><td>세종대학교 광개토관 B1</td></tr>
<tr><td rowspan="4">참석자</td><td>사회</td><td colspan="2">배정철(부산대학교 겸임교수, 동의대학교)</td><td>발제 이예림(주식회사 업폴 대표)</td></tr>
<tr><td rowspan="3">패널</td><td colspan="2">염세경(동국대학교 산업시스템공학과 교수)</td><td>민재명(한국열린사이버대하교 교수)</td></tr>
<tr><td colspan="2">이진(사이버보안연구소 소장)</td><td>윤성열(사이버정책청년연구회 회장)</td></tr>
<tr><td colspan="2"></td><td></td></tr>
</table>

<table>
<tr><td>제안내용</td><td>디지털 트윈 기술은 디지털 전환(DX)을 넘어 AI 전환(AX) 시대의 핵심 요소로 급부상하며, 빅데이터 및 인공지능 기술의 발전과 함께 그 가치를 증대시키고 있다. 3D 모델링, 공간정보(GIS), BIM, IoT 센서, 5G 통신 등 관련 기술의 성숙으로 실제 도시, 공장, 나아가 인간 장기까지 폭넓게 구현되며 스마트시티, 디지털 헬스케어, 생산 및 물류 최적화 등 기존 시스템의 효율성을 크게 높일 잠재력을 가지고 있다.
그러나 이러한 디지털 트윈 기술의 발전은 혁신 이면에 다양한 법적, 사회적, 윤리적 문제들을 야기하며, 이에 대한 심도 깊은 논의와 책임 있는 대응이 시급하다. 특히, 초연결된 실시간 데이터 수집 및 활용으로 인한 개인정보 침해(행동 패턴, 건강 상태, 동선 등 민감 정보 집약) 및 대규모 유출의 위험성이 커지고 있다. 또한, 가상 환경 시뮬레이션 및 예측된 결과가 현실 왜곡을 초래하거나 실제 인명 피해와 같은 부정적 영향을 미칠 경우, 이에 대한 책임 소재가 불분명하다는 문제가 제기된다. 이 외에도 구축된 공간정보의 개방 및 활용에 따른 저작권 침해 문제, 그리고 생성되는 방대한 데이터의 윤리적인 활용과 보호 방안 등 복합적인 과제들이 산적해 있다.
본 세션은 디지털 트윈 기술의 긍정적 영향과 함께 이로 인해 발생하는 핵심적인 법적, 사회적, 윤리적 문제들을 다자간 관점에서 심도 있게 논의하고, 지속 가능한 기술 발전과 함께 예측 불가능한 위험에 대한 명확한 책임 구조를 정립하며, 사회적 합의와 협력을 통한 디지털 거버넌스 구축 방안을 모색하고자 한다. 이 과정에서 다양한 이해관계자들의 참여를 통한 제도적, 정책적 지원 방향 또한 논의할 것이다.

◎ 주요 쟁점
1. 디지털 트윈을 통한 방대한 실시간 데이터 수집 및 활용이 개인의 프라이버시와 데이터 보안에 미치는 영향은 무엇이며, 이를 효과적으로 보호할 방안은 무엇인가?
2. 디지털 트윈 시뮬레이션 및 예측값이 현실에 부정적인 영향을 미치거나 사고를 유발했을 때, 그 책임(기술 개발자, 운영자, 사용자 등)을 어떻게 명확히 규정할 수 있는가?
3. 급변하는 디지털 트윈 기술 발전에 대응하기 위해, 유연하고 견고한 거버넌스 체계를 어떻게 구축하며, 특히 다양한 이해관계자(정부, 산업계, 학계, 시민사회, 기술 커뮤니티, 청년 등)의 실질적인 참여를 어떻게 확대할 것인가?
4. 디지털 트윈 시대에 개인의 데이터 통제권을 실효적으로 보장하고, 영업비밀 등 민</td></tr>
</table>

	감 정보의 보안을 강화하기 위한 기술적/제도적 해법은 무엇인가?
요약내용	'혁신과 책임의 경계에 선 디지털 트윈 기술의 두 얼굴과 미래'를 주제로, 디지털 트윈 기술의 현황과 미래 방향, 그리고 수반되는 윤리적·법적 문제들을 심층적으로 다루었다. 디지털 트윈이 단순한 복제 기술을 넘어 우리의 삶과 정책, 윤리적 경계까지 흔들고 있는 현상을 강조했다. 발제는 디지털 트윈 기술이 현재 어떻게 구현되고 있는지, 우리가 주목해야 할 핵심 키워드, 그리고 예방을 위해 정확히 알아야 할 문제점들을 포괄적으로 다루었다. 디지털 트윈의 핵심을 빅데이터, AI, 3D 모델링 시뮬레이션으로 요약했다. 특히, AI가 방대한 데이터 학습을 통해 응답하며, 이 데이터를 잘 조직하고 시스템 모델링으로 3D화하여 시뮬레이션하는 것이 디지털 트윈의 본질임을 설명했다. 최신 트렌드로는 공간지능(Spatial Intelligence)과 피지컬 AI(Physical AI)를 언급하며, 2D 이미지만으로 3D 생성이 실시간으로 이루어지는 기술 발전과 로봇 훈련 및 자율주행 기술(테슬라 FSD)의 발전을 소개했다. 그러나 이러한 기술 발전 이면에는 데이터 부족으로 인한 사고 시나리오 시뮬레이션의 한계, 현실 왜곡 가능성, 그리고 책임 소재의 불명확성과 같은 심각한 문제점들이 내재되어 있음을 지적했다.
논의 세부 내용	1. 세션 소개 및 디지털 트윈 기술의 현황과 미래 본 세션은 "혁신과 책임의 경계에 선 디지털 트윈 기술의 두 얼굴과 미래"라는 주제로, 현재 정부가 추진하는 글로벌 AI 3대 강국 정책과 디지털 기술 변곡점에 서 있는 시점에서 디지털 트윈 기술에 대한 심도 있는 논의의 장을 마련했다. 사회를 맡은 배정철 동의대학교 교수는 디지털 트윈이 단순한 복제 기술을 넘어 인간의 삶, 정책, 윤리에 광범위한 영향을 미치고 있음을 강조하며, 기술이 나아갈 방향에 대한 진지한 성찰의 필요성을 역설했다. 발제는 업폴의 이예림 대표가 맡아 '디지털 트윈 기술: 혁신인가, 위험인가, 미래를 위한 선택'이라는 제목으로 진행되었다. 이 대표는 디지털 트윈의 현 상황과 적용 사례, 그리고 우리가 주목해야 할 핵심 키워드를 제시하며 발표를 시작했다. • 디지털 트윈의 핵심 키워드: 이 대표는 디지털 트윈을 이해하기 위한 세 가지 핵심 키워드로 빅데이터, AI, 3D 모델링 시뮬레이션을 꼽았다. 특히, AI의 응답은 그 뒤에 숨어있는 수많은 데이터에 기반하며, 데이터를 잘 조직하고 AI에 반영하는 것이 중요하다고 설명했다. • 공간지능의 중요성: 컴퓨터 비전 및 AI 분야의 권위자인 페이페이 리 교수가 언급한 '공간지능(Spatial Intelligence)' 개념을 소개하며, 미래 AI는 물질 세계를 이해하는 AI 모델을 기반으로 할 것이라고 강조했다. 이는 2D 이미지만으로 3D 객체를 생성하는 오디세이 AI와 같은 기술의 발전을 통해 실시간으로 모든 것이 생성되는 디지털 트윈의 가능성을 보여준다. • 피지컬 AI 및 산업 적용: 아마존 로봇의 100만 대 돌파 사례를 통해 물리적 AI(Physical AI)의 중요성을 설명했다. 엔비디아의 '옴니버스 디지털 트윈' 기술처럼, 로봇들이 가상공간에서 수많은 시뮬레이션을 통해 훈련함으로써 실제 물리적 환경에서의 학습 시간을 단축할 수 있다고 언급했다. • 디지털 트윈의 역기능과 한계: 이 대표는 기술의 긍정적 측면과 함께 부정적 영향에 대한 우려를 제기했다.

	○ 테슬라 FSD 사고 사례: 테슬라의 완전 자율주행(FSD) 기능이 켜진 상태에서 일가족이 사망한 사건을 예로 들며, 디지털 트윈 기반 학습의 한계와 데이터 부족 문제를 지적했다. 사고 시나리오에 대한 데이터와 시뮬레이션 환경이 충분히 조성되어 있지 않은 점이 실제 인명 피해로 이어질 수 있음을 경고했다. ○ 책임 소재의 불명확성: 이러한 사고 발생 시, 학습 모델, 테슬라 회사 전체, 혹은 운전자 중 누구에게 책임이 있는지 불명확하다는 점을 문제 삼았다. ○ 개인정보 침해 위험: BMW 사례를 통해 작업자의 동선이나 개인정보가 디지털 트윈 구축 과정에서 누락될 수 있음을 언급하며, 초연결된 실시간 데이터 수집 및 활용으로 인한 프라이버시 침해와 대형 유출 위험을 경고했다. 특히, 개인의 행동 패턴, 건강 상태, 동선 등 민감한 정보가 디지털 트윈 안에 집약될 때 발생하는 문제에 대한 고민이 필요하다고 강조했다. 이 대표는 이러한 문제점들에 대한 깊은 논의를 통해 데이터의 효과적인 관리와 문제 발생 전 예방할 수 있는 방안을 모색해야 한다고 제안했다. 또한, 소버린 AI의 발전을 통해 데이터와 기술이 소수의 힘 있는 주체(국가 또는 기업)에게 집중되는 현상 속에서, 한국이 도태되지 않기 위해 어떤 방식으로 참여하고 발전해야 할지에 대한 질문을 던지며 논의를 이어갔다. 2. 디지털 트윈 기술에 대한 다자간 관점 이예림 대표의 발제에 이어, 각 분야 전문가들이 디지털 트윈 기술의 혁신과 책임에 대한 다양한 관점을 제시하며 열띤 토론을 펼쳤다. • 염세경 교수 (동국대학교 산업시스템공학과, 기술계): 염세경 교수는 본인의 연구 분야인 인간공학 및 헬스케어에서의 경험을 바탕으로, 윤리적 규제와 연구 현실 간의 괴리를 지적했다. IRB(기관생명윤리위원회) 승인 과정의 어려움과 데이터 수집의 난항을 언급하며, 이는 기술 발전 속도를 늦추거나 현실적으로 필요 없는 기술을 만들게 할 수 있다고 우려했다. 특히, 인공지능 분야에서 한국 기술력이 중국에 밀리는 현상을 언급하며, 우리가 책임을 논할 만큼 기술을 개발해본 적이 있는가라는 도발적인 질문을 던졌다. 기술은 항상 위험성을 내포하지만 (예: 초기 자동차 사고), 사람을 살리는 기술이 될 수도 있음을 강조하며, 규제보다는 기술 개발에 대한 과감한 투자를 주장했다. 또한, 개인 데이터 소유권과 관련하여 자신의 경험을 예로 들며, 개인 데이터 제공에 대한 적절한 보상과 투명한 커뮤니케이션이 이루어진다면 연구자들이 데이터를 더 쉽게 확보할 수 있을 것이라는 아이디어를 제시했다. • 민재명 교수 (한국열린사이버대학교, 학계): 민재명 교수는 혁신과 책임의 관점에서 '먹고사는 문제'를 넘어 '죽고사는 문제'로 변화한 위험성과 이에 대한 사회 전반의 인식 변화가 필요하다고 강조했다. 과거 과학자들에게 국경이 없었으나, 이제는 군인과 유사한 인식적 변화가 필요한 시기가 되었다고 진단했다. 소버린 AI와 관련된 대규모 투자의 필요성을 언급하며, 탁상공론에 그친다면 후손들의 미래에 대한 책임감 있는 선택이 될 수 없다고 비판했다. 윤리와 도덕은 시대에 따라 변화해왔으므로, 기술 발전을 가로막는 대상이 되어서는 안 된다고 주장했다. 한국 사회가 IT 기술 발전 과정에서 충분한 통제 역량을 입증했음을 믿으며, 폭넓은 기술 허용이 필요하다는 입장을 밝혔다. 또한, 디지털 트윈 기술이 국민들이 체감할 수 있도록 행정에 빠르게 도입되어야 한다고 주장했다. 온라인 인감 발급의 예시를 들며, 제도적 미비로 인해 여전히 불필요한 행정 절차가 반복되는 현실을 지적했다. 데이터 연동과 간소화를 통해 행정 효율을 높이고, 복지 사각지대 해소를 위한 '따뜻한 기술'로 나아가야 한다고 역설했다.

	• 이진 소장 (사이버안보연구소, 시민사회): 이진 소장은 과거 SF 소설에서 상상하던 내용들이 기술적으로 현실화되고 있음을 언급하며, 문제점 또한 상상 가능하다고 보았다. '월드 오브 탱크' 게임을 비유로 들어, 디지털 트윈이 물리적 법칙을 동일하게 적용하는 세상이라면, 데이터의 공개 범위와 보안이 핵심 문제라고 설명했다. 특히 방산 산업의 영업비밀과 같은 민감한 데이터는 노출되어서는 안 되며, 플랫폼 내에서 데이터가 암호화되고 외부에 노출되지 않는 기술적 보장이 필요하다고 강조했다. 엔비디아의 옴니버스 같은 플랫폼이 모든 데이터를 집적할 가능성에 대한 우려를 표하며, 기업이나 국가 차원에서는 최소한 자기 데이터 보안을 어떻게 할지 상상하고 준비해야 한다고 주장했다. 또한, 개인정보는 이미 대다수가 알게 모르게 여러 회사에 제공되어 '존재하지 않는' 현실임을 지적하며, 이는 자본주의 사회에서 서비스 이용의 대가로 감내하는 측면이 있다고 보았다. 이러한 상황에서 기술적으로 '제로 트러스트(Zero Trust)' 개념을 적용하여, 서로 신뢰할 수 없는 환경에서도 안전하게 데이터를 교환할 수 있는 시스템을 구축하는 것이 해법이라고 제시했다. 이는 컨소시엄 블록체인 형태로 권한을 나누고 모든 데이터를 기록하여, 불순한 의도의 행위에 대한 증거를 남김으로써 책임을 물을 수 있는 구조를 제안했다. 그는 규제 방식에 대해서도 법에 없는 것은 일단 할 수 있게 하고, 문제가 발생하면 그에 대한 규제를 추가하는 '선 허용-후 규제' 방식으로 전환해야 한다고 주장했다. • 윤성열 회장 (사이버안보정책청년연구회, 청년): 윤성열 회장은 본인의 주 연구 분야인 국제관계학 및 국토안보 연구를 바탕으로, 과거 국방안보 중심에서 최근 사이버안보가 국토안보의 중요 영역으로 부상했음을 언급했다. 기술 발전 속도에 비해 법적·제도적 부분이 뒷받침되지 못하는 현상을 지적하며, 디지털 트윈 분야는 민간보다는 국방 영역에서 더욱 중요하게 다루어져야 한다고 주장했다. 특히, 국방 및 국가안보 차원에서 AI 기술의 독립성과 신뢰성 확보가 핵심 과제임을 강조했다. 그는 디지털 트윈 분야의 정책과 제도 마련을 위해 '책임 있는 혁신' 원칙을 설정해야 한다고 제안했다. 이 원칙에는 ▲안전성, 윤리성, 사회적 수용성 우선, ▲공공의 이익 최우선, ▲기술의 접근성 및 포용성 (사회적 약자 혜택), ▲투명성 (기술 영향, 데이터, 알고리즘, 예측 결과 공개) 등이 포함되어야 한다고 밝혔다. 또한, 디지털 트윈 시대의 프라이버시권 재정의가 필요하며, 개인이 자신의 디지털 트윈 생성 데이터를 소유, 통제, 삭제할 수 있는 권리를 법적으로 명문화해야 한다고 주장했다. 민간 영역의 디지털 트윈 연구를 위해 개인 영역 정보는 학계 연구자들에게 공개될 필요가 있다고 보았다. 마지막으로, 산학연군 연계를 통한 다학제적 거버넌스 구축을 통해 미래전에 대비해야 한다고 역설했다. 3. 주요 쟁점에 대한 심층 논의: 책임 소재 및 데이터 관리 방안 3-1. 예측 기반 결정 및 사고 발생 시 책임 소재의 명확화 사회자는 불분명한 책임 구조가 기술 수용의 걸림돌이 될 수 있음을 지적하며, 예측 기반 결정 및 사고 발생 시 책임 소재를 명확히 할 방안에 대한 논의를 요청하였다. • 염세경 교수는 책임 소재 결정의 어려움을 토로하며, 기업, AI 개발자, 운전자 등 다양한 주체가 존재한다고 언급하였다. 염 교수는 궁극적으로는 기술을 사용하는 '사용자의 몫'이 될 수 있다고 보았다. 자동차 사고의 예를 들며, 기술 사용의 편리함을 누리는 대가로 개인이 일정 부분 위험을 감수해야 할 필요성을 제기하였다. 또한, 개인 데이터 제공과 관련하여 자신의 경험을 예시로 들며, 적절한 보상과 투명한 커뮤니케이션이 이루어진다면 연구자들이 데이터를 더 쉽게 확보할 수 있을 것이라는 아이디어를 제시하였다. 염 교수는 책임 소재가 덜 불분명한 분야부터 기술을 적용해 나가는 것이 바람직

	하다는 의견을 덧붙였다. 3-2. 데이터 활용 투명성 및 개인의 통제권 확보 청중은 데이터 사용 승인 시 투명성이 부족하고 개인에게 책임감이 전가되는 문제에 대한 우려를 표명하며, 기관의 투명성 보장 방안을 문의하였다. • 염세경 교수는 데이터 사용 승인이 맹목적이지 않으며, 투명성은 제공되나 사용자의 '불신'이 문제의 핵심이라고 응답하였다. 개인이 기술 사용 여부를 선택하는 문제이며, 기존 제도적으로 투명한 절차가 존재함에도 불구하고 인식 부족과 활성화 미비가 문제라고 지적하였다. 데이터 제공에 대한 보상(예: 커피 쿠폰, 치아 데이터 사용 시 3,000원 적립)을 통해 개인의 동기를 유발할 수 있다고 제안하였다. • 이진 소장은 "여러분 개인정보는 존재하지 않습니다"라는 발언으로 답변을 시작하며, 우리가 홈쇼핑 등 일상 서비스 이용을 위해 빈번하게 약관에 동의하고 있으며, 이 과정에서 개인정보가 자회사 등 광범위하게 공유되는 것이 현실임을 지적하였다. 소장은 이러한 자본주의 사회에서 서비스 이용의 대가로 개인정보 제공이 불가피한 측면이 있다고 보았다. 따라서 개인정보 보호에 집중하기보다는, 기업의 영업비밀 및 국가 경쟁력 보호와 같은 영역에 집중해야 할 필요성을 강조하였다. 4. 지속 가능한 디지털 거버넌스 구축을 위한 사회적 협력 4-1. 기술 발전 속도에 대응하는 거버넌스 체계 구축 사회자는 기술 발전 속도에 대응 가능한 유연하고 견고한 거버넌스 체계 구축의 필요성을 강조하며, 특히 정부, 산업계, 기술 커뮤니티, 시민사회 간의 다자 간 협력 구조 도입의 시사점에 대한 논의를 요청하였다. • 윤성열 회장은 학계에서는 거버넌스에 대한 논의가 활발하지만, 기술의 궁극적인 수혜자인 '시민'과 '국민'의 직접적인 의사결정 참여가 중요하다고 강조하였다. 그는 도시 개발과 같은 분야에서 시민 위원회 구성이나 대국민 공론의 장 마련을 통해 일반 시민이 거버넌스 현장에 적극적으로 참여할 수 있도록 해야 한다고 제안하였다. 이는 디지털 트윈에 대한 흥미를 유발하고 대국민 공감대를 형성하는 데 기여할 수 있을 것이라고 언급하였다. • 민재명 교수는 마드리드 루미오와 같은 시민 의사결정 플랫폼의 해외 사례를 언급하며, 국내에서도 시민 참여 노력이 있었으나 충분한 효과를 거두지 못했다고 지적하였다. 그는 현재 공론장의 기능이 유튜브 등으로 분산되어 건강한 담론 형성의 어려움이 있다고 보았다. 미국의 싱크탱크 생태계를 예시로 들며, 정책 경쟁 및 건강한 순환 구조를 위한 제도적 개선이 필요하다고 강조하였다. 민 교수는 제도적 기반 없이 이루어지는 논의는 '허공에 그림을 그리는 것'과 같아 무의미할 수 있다고 비판하였다. • 이진 소장은 한국의 규제 방식에 대한 근본적인 변화를 주장하며 '선 허용-후 규제' 방식으로의 전환을 제안하였다. 현재 한국은 법에 명시되지 않은 것은 불법으로 간주하는 자기검열이 만연하여 혁신이 저해되고 있다고 지적하였다. 이러한 규제 방식에 대한 인식 변화가 데이터 확보 및 시스템 개발에 필수적이라고 강조하였다. 4-2. 실시간 융합 데이터의 법적 포괄 및 통제권 보장 사회자는 디지털 트윈 구현 과정에서 방대한 실시간 융합 데이터가 생성되는 것이 새로운 법적·윤리적 과제를 야기한다며, 현행 개인정보보호법이 이러한 데이터를 제대로 포괄할 수 있는지, 그리고 데이터 통제권을 실효적으로 보장할 방안에 대해 질문하였다. • 민재명 교수는 데이터 3법 및 마이데이터 사업 등 기존의 제도적 기반이 존재하며, 비식별화, 가명처리 등 기술적 보호 조치를 통해 개인정보를 보호하면서도 데이터 활용

	이 가능하다고 설명하였다. 민 교수는 책임을 특정 주체에게 전가하기보다 사회 전체가 공통으로 논의하고 수용하며 즉시 대응하는 것이 중요하다고 강조하였다. AI 규제 또한 저작권 논의처럼 지속적인 대화와 유연성을 통해 접근해야 한다고 보았다. • 이진 소장은 한국의 CCTV 사례를 통해 국민들이 안전이라는 대가로 개인정보 침해를 일정 부분 감수하고 있음을 지적하였다. 그는 기술이 발전할수록 개인의 프라이버시 침해는 증가할 수밖에 없으며, 중요한 것은 이로 인한 이익이 얼마나 공정하게 분배되는가에 집중해야 한다고 보았다. 현행 개인정보보호법이 '문구적'이며 실효성이 부족하다고 비판하며, 법이나 제도로 해결하기 어려운 부분은 기술로 직접 구현하고, 그 과정에서 발생하는 문제점을 점진적으로 개선해 나가는 방식이 필요하다고 제언하였다.
워크숍 총평	- 디지털 트윈 기술의 현황과 미래, 그리고 그로 인해 야기되는 복합적인 법적, 사회적, 윤리적 문제들을 다자간 관점에서 심도 있게 논의함. - 구체적인 사례를 통해 디지털 트윈 기술의 역기능과 데이터 부족, 책임 소재의 불명확성 등 현실적인 과제들을 명확히 제시함. - 기술 개발의 윤리적 규제와 현실 간의 괴리, 한국 기술력의 현주소에 대한 성찰, 개인 데이터 소유권과 보상의 필요성 등 기술계, 학계, 시민사회, 청년 등 다양한 이해관계자들의 관점을 나눔. - 예측 기반 결정 및 사고 발생 시 책임 소재를 명확히 하고, 데이터 활용의 투명성을 확보하며, 개인의 통제권을 보장하는 방안에 대한 깊이 있는 논의함. - 급변하는 기술 발전 속도에 대응 가능한 유연하고 견고한 거버넌스 체계 구축의 중요성이 강조되었으며, 시민/국민의 직접적인 의사결정 참여 확대, '선 허용-후 규제' 방식의 전환, 그리고 실효성 있는 데이터 보호를 위한 기술적 구현 등 다양한 정책적, 제도적 제언들을 제시함. - 기술 발전의 양면성을 인지하고 예측 불가능한 위험에 대한 명확한 책임 구조를 정립하며, 지속 가능한 디지털 거버넌스를 구축하기 위한 사회적 합의와 협력의 중요성에 대한 공감대를 형성함

2025 한국인터넷거버넌스포럼(KrIGF) 워크숍 세션 보고서

작성자 : 고아침

세션명	<AI 윤리 레터> 성과보고를 통해 살펴보는 한국 AI 윤리 대중담론의 현재와 미래			
일시	2025. 7. 3. (목), 15:10~16:10		장소	세종대학교 광개토관 B1
참석자	사회	고아침(AI 윤리 레터 운영진)	발제	고아침(AI 윤리 레터 운영진)
	패널	권오현(사회적협동조합 빠띠)		송수연(언메이크랩)

제안내용	<AI 윤리 레터>는 AI 윤리 및 AI의 사회적 맥락을 다루는 뉴스레터로, 2023년 5월부터 운영되고 있습니다. 한국어로 AI 윤리를 중점적으로 다루며 한국의 AI 윤리 이슈에 주목하는 사실상 최초의 대중적 커뮤니케이션 채널로, 테크업계 / 시민사회 / 학계 등 다양한 배경의 구성원이 필진으로 참여하여 주 2회 발송하고 있습니다. 이에 더해 <AI 윤리 레터>는 공개 읽기 모임/워크숍/세미나/기고/발표 등 국내외 활동, AI 분야 젠더 편향을 살펴보는 인터랙티브 스토리텔링 프로젝트, LLM 데이터셋을 비판적으로 리뷰하는 인터랙티브 툴, 제21대 대선을 둘러싼 AI 정책 담론 분석 연재 등 다양한 형식의 활동을 펼쳐왔습니다. 이 과정에서 AI 윤리 관련 개념/데이터셋/도구, 국내외 AI 정책 및 거버넌스, 업계 동향 및 AI 하이프, 데이터 권리 및 노동 이슈, 차별, 오정보, 감시, 폭력, 기후/환경, 전쟁 등 폭넓은 주제를 다뤘습니다. 이러한 활동의 지향점은 이론, 기술, 실천이 만나는 공간으로서, 시민사회, 기술업계, 학계, 문화예술, 공공/정부 등 다양한 영역을 연결하고자 함입니다. 나아가 한국의 AI 윤리 및 비판적 기술 담론의 대중적 커뮤니케이션에 기여하는 것을 목표로 하고 있습니다. 이를 위해 AI 윤리 북클럽을 운영하는 등 커뮤니티 활동을 겸하고 있습니다. 본 세션에서는 2년 남짓 본 프로젝트를 운영해오며 달성한 소기의 성과와 얻게 된 인사이트를 공유하고, 사례 중심으로 한국 사회 AI 윤리 대중담론 지형의 윤곽을 그립니다. 나아가 사회적으로 유의미한 AI 윤리 담론 형성 및 대중 커뮤니케이션을 위한 제언과, 한국 사회를 넘어서 국제적 논의 및 연대의 가능성을 제안합니다.
요약내용	• AI 윤리 레터 취지 및 운영 현황을 설명하여 개요를 제시함 • 뉴스레터가 다뤄온 주요 주제 및 사례로는 노동 착취, 젠더 편향, 데이터 권리, 허위정보, 생태 영향, 기술 거버넌스, 문화적 영향, 감시 기술 등이 있음 • 뉴스레터를 운영하며 관찰한 주요 추세로는 '존재론적 위협' 류의 AI 하이프가 현실적 폐해를 가리는 효과, 그리고 AI 국가주의 확산 및 기술 산업에 치중한 담론 불균형이 있음 • 비판적 대안 제시를 원하는 목소리는 적지 않지만 단절되어 있음. 이에 다양한 목소리를 연결하고, 기술 리터러시를 확산하며, 한국 맥락에서 정책과 담론 논의를 치열하게 가져갈 필요 있음 • 기술적 접근 다양성, 비판적 담론 형성, 공동체 중심 기술 설계 등을 키워드로 패널 토론 진행

논의 세부 내용	1. 발제 요지 <AI 윤리 레터> 활동 요약 • AI 윤리 레터는 2023년 5월 창간된 한국어 AI 윤리 전문 뉴스레터로, 기술·정치·사회적 담론을 아우르며 국내외 AI 윤리 이슈를 집중 조명한다. • 한국 최초로 AI 윤리를 전문적으로 다루는 콘텐츠 채널 • 인공지능 기술의 산출물과 사회적 영향을 윤리적 관점에서 분석하고, 다양한 분야(공학, 사회학, 인문학)의 논의를 연결하며 특정 기술적 문제(예: 데이터셋 분석)부터 사회적 맥락(예: 젠더 담론, 기후 변화)까지 아우르고자 함 • 기술정치 관점에서 AI 기술의 기획, 생산, 활용 전 과정의 윤리적 문제를 다룸 • 주 2회 발송되며, 현안 브리핑과 에세이를 통해 데이터 권리, 노동 문제, 기술 거버넌스, 젠더 편향, 기후 영향, 허위 정보 등 다양한 주제를 다룬다. • 발표 시점 기준 필진 8명이 참여하며, 170회 발송, 글 400여 편 작성, 구독자 1,600명(오픈율 40%), 독자 피드백 100여 건 기록 중 • 책읽기모임 'AI 윤리 북클럽'에서 파생된 프로젝트로, 느슨한 커뮤니티 기반으로 운영된다. 주요 주제 • 노동: 케냐 데이터 라벨링 노동자의 저임금·심리적 피해, AI로 인한 일자리 대체 문제 등 • 젠더/소수자 편향: 국내 AI 기업 행사 연사 성비 88:12로 드러난 성별 불균형을 살펴본 인터랙티브 스토리텔링 프로젝트, 이미지 생성 기술의 성 편향 재생산 이슈 등 • 감시 기술: 국가 감시 시스템과의 연계, 전쟁 기술로서의 AI • 데이터 권리: 플랫폼의 약관 개정으로 인한 사용자 데이터 무단 활용 논란 등 • 허위 정보: 생성형 AI 기술 발전으로 선거 기간 허위 정보 확산 우려 등 • 환경 영향: 에너지 집약적 AI 기술의 탄소 배출 및 데이터센터 확장 문제 • 기술 거버넌스: 국내 AI 기본법 논의, 대선 공약에서의 AI 정책 검토 • 문화적 영향: 지브리 스타일 생성 기능 열풍과 예술적 창의성 침해 논란 • 학술 인접 활동: AI 윤리 분야 컨퍼런스인 FAccT 논문 다이제스트, 네이버의 AI 윤리 데이터셋 분석하는 인터랙티브 툴 제작 • AI 만능론/공포를 부추기는 'AI 하이프 뉴스'를 식별하기 위한 체크리스트 번역 소개 • 그밖에 공개 읽기 모임, 워크숍, 세미나, 발표, 기고, 정책 논의 등 외부 협력 활동 진행 뉴스레터 운영 과정에서 관찰한 추세 • 존재론적 위협 vs. 현실적 해악: AI의 인류 멸종 위협 논의는 기술 업계 과대평가와 규제 완화로 이어졌으나, 노동 착취·젠더 편향 등 현실적 해악이 방치되고 있음. • AI 국가주의 확산: 기술 경제 성장과 안보 자산으로서의 AI 강조로 산업 진흥 정책이 우선시되며, 사회적 가치 논의가 소외됨. • 담론 불균형: 기술 산업 중심의 담론이 지배적이며, 시민사회와 인문학적 관점이 배제되거나 표면적 논의에 머무름. 주요 도전 과제 • 자원 부족: 공개 운영 여력 부족으로 알음알음 운영되는 비공개 커뮤니티의 한계 • 산업 중심 담론: AI 국가주의(경제 성장·안보 우선)로 인한 윤리적 논의의 주변화 • 다양성 부족: 기술 업계의 일방적 성장 서사에 맞서 다양한 목소리를 통합하는 데 어려움 뉴스레터 활동의 장기적 지향점 및 제언 • 기술 전 생애 과정에서 다양한 목소리 연결하고 시민·학계·예술·문화 영역 간 교류 채널 구축이 필요함 • 기술 리터러시 확산하여 AI 기술의 사회적 영향 인식 제고 및 대안 모색 공감대 형성 • 정책 개선: 산업 진흥과 사회적 가치의 균형, 데이터 권리 보호, 젠더·노동·환경 문제 반영 등 • 실리콘밸리 중심 기술 담론에서 벗어나 한국적 맥락, 지역 사회 특성과 요구를 반영한 논의 필요.

	• 기술결정론을 지양, 공익적이고 정의로운 방향으로 기술을 함께 설계해가는 공동체적 실천이 요청됨 2. 토론 요지 송수연: 비판적 대안에 관심이 있는 사람으로서 참여. AI 윤리 레터가 그동안 많은 주제를 다뤘고 시의적인 쟁점을 발굴해온 것이 중요한 성과. 기술을 공학적으로 이해하는 것도 중요하지만 사회적, 문화적인 맥락에서 은유적으로 또 비판적으로 접근하는 것도 가능. 다양한 해석과 비판의 축적과 교차가 대중적인 담론이 시작되는 중요한 힘이 된다. AI 윤리 레터의 작업 과정과 질문이 대중과 만나는 과정이 중요한 이유도 비판적 기술 담론의 다층화. 기술적 현안에 대해 사회적 응답이 필요할 때 여러 관점에서 볼 수 있도록 목소리가 다양해질 필요가 있다. 저는 매년 예술 종사자들과 함께 중요한 기술 이슈를 하나 정하고, 작은 담론의 자리를 기획해오고 있다. 그런 논의 자리가 많지만, 예술 분야에서 자리를 만든다는 것이 의미가 있다. 하지만 진행할 수록 기술, 사회, 예술의 접점에서 담론의 자리가 어떤 형태로 존재할 수 있을지 고민은 계속된다. 기술에 관해 비판적인 관점을 가진 사람들이 많다고 했는데 그들이 개별의 경험, 공통의 경험을 서로 순환시키고 유기적으로 연결할 수 있는 활동으로 무엇을 할 수 있을까? 그것이 한국의 맥락 위에서 시작된다면 어떤 것이면 좋을지? 고아침: 말씀하신 <포킹룸> 같은 기획, 문화예술 영역에서 운영되는 커뮤니티 활동도 중요한 사례이고, 학술적인 논의의 장이나 언론 매체 같은 담론 공간이 분명 활발히 작동하고 있다. 그런데 학술/언론 같은 전통적 공간이 다양한 목소리를 충분히 효과적으로 담아내고 있느냐는 의문의 여지가 있고, 결국 새로운 접근이 추가되어야 하는데 그것이 무엇일지 답을 찾고 있는 단계. 뉴스레터는 북클럽에 기반한 느슨한 커뮤니티로 활동하고 있고 딱히 적극적으로 홍보를 하고 있지는 않은 상황. 개인적으로 더 가시화하는 방법을 찾아봐야 할까, 예를 들어서 형식을 갖춘 단체를 조직해서 기존의 네트워크에 더 깊숙이 진입하는 활동이 필요할지 고민 중. 권오현: AI 윤리 레터가 AI에 대한 담론 불균형 상태인 한국에서 개선을 하려는 노력을 했고 중요한 아젠다를 많이 다뤘다. 의미 있는 노력인 한편 AI 국가주의라고 표현한 현실도 있다. 한국의 발전을 위해서 AI는 무조건 해야 하는 상황, 우리가 전 세계에서 AI 3대 강국을 어떻게든 만들어야 한다는 전제 하에 온 국민들이 휩쓸려가고 있는 상황. 마치 땡볕 아래서 물을 뿌리고 있는 듯한 느낌도 있다. 그게 의미가 없다고 보지는 않는데, 흔히 주류 기술 담론의 배후에 있는 사람으로 많이 지목되는 피터 틸 같은 사람이 제로(0)보다 원(1)이 되면 엄청난 큰 가능성이 있는 거다라고 이야기하는 부분에서 저는 중요한 가능성을 본다. 그럼에도 불구하고 냉정하게 보아 담론의 불균형 상태가 1에서 10 사이 어디에 있다고 느끼시는지 궁금하다. 다양한 목소리들을 우리가 담아내자. AI 만능론, 모든 것을 해결해줄 수 있는 AI(에 관한 논의)가 되어 버린 상태에서 반대편의 논의는, 규제나 소비자 권리를 주장하는 수준을 넘어서는 담론을 어떤 형태로 호명할 수 있을까? 어떤 기술들이 공동체에 어떻게 기여하고, 또 공동체가 가지고 있는 생태적인 한계 안에서 어디까지 발전시켜야 하고, 기술을 특정 빅테크가 아니라 시민들이 공동으로 소유하고, 이런 형태들을 우리가 뭐라고 부를 수 있을까? 이런 논의를 단순히 '다양한 목소리'라고 퉁칠 게 아니라 그것들의 이름을 짓고 담론을 만들어나갈 가능성이 보이는지 궁금하다. AI 의인화, 인간으로 표현이 된 기술 뒤에 사람이 있다고 지적했는데 궁극적으로 사람들이 가지고 있는 가치들이 충돌하고 있는 것 같다. AI 만능론을 추구하는 사람들이 AI 뒤에 숨어서 여러 가지 가능성을 약속하고 있는데 그 가치와 다른, 시민들이 추구하는 다른 가치는 어떤 이름을 붙일 수 있을지 궁금하고, 그런 가치를 막연하게 느끼면서 현실을 인내하고 답답해하고 비판적 대안에 관심을 가진 사람들을 어떻게 모을 수 있을까? 이런 것들이 중요한 과제. 고아침: 일단 담론적인 불균형은 1인 것 같다. 현실에 영향을 거의 못 주고 있다고 생각. AI 만능론은 몇 가지로 쪼개서 생각해볼 수 있는데 핵심적인 요소 하나는 GPT 등에서 확인되는 거대 모델 만능론이라고 치환할 수 있다. 데이터를 때려넣고 GPU를 엄청 돌려서 만든 모델이 생각보다 성과가 잘 나오고, 그런 추세가 계속될 것이라는 전제에 다

	들 세게 배팅하고 있는 상황. 과연 그러할 것인지는 생각해볼 문제. 한국에서도 AI 고속도로라는 이름으로 데이터센터 구축 예정인데 잘되면 좋겠지만 만약 생각보다 빠른 시점에 기술 성장의 한계나 천장에 부딪힌다고 하면 산업적으로도 판단 미스가 될 위험이 있다. 경제 성장만 좇지 말고 인권도 챙기자는 것도 너무 중요한 이야기이지만 동시에 기술에 접근하는 방식 자체의 다양성 또한 필요하다. AI 기술의 수혜가 무엇인지, 관념 자체를 재정의할 필요가 있다. 한국의 소버린 AI를 만들어서 어느 기업이 잘 만든 상용 서비스를 한국 국민이 모두가 쓰면 그게 공익적인 것인지? 이런 관념에 균열을 내는 작업이 필요한 것 같다. 단지 사이즈를 키워서 성능을 키우는 언어 모델 같은 하나의 접근 방식 말고, 맥락 특정적이거나 특정한 문제 해결에 적합한 솔루션들이 무엇인지, 모델 사이즈를 키우면 원툴로 다 되는 것인지, 이런 논의가 더 필요하다. 권오현: AI 발전에 노력을 기울이지 말자는 이야기는 조심스러운 것이 맞다. 하지만 AI나 AI 기술 이전 정보화 기술이 GDP 성장에 정말 기여를 했냐, 이런 목소리도 있다. 그러지 못할 가능성에 대해서도 공동체는 같이 보험을 들듯이, 다양한 시도와 관점을 가지고 준비해야 하는 것 같고, 정말 우리가 기술을 가지고 뭘 할 것인지, 우리 공동체를 위해서 어떤 이득을 줄 것인지에 관한 논의도 늘어나는 계기가 생기기를 기대한다. 송수연: 기술 접근 방식의 다양성이 필요하다는 말에 공감. 생성형 인공지능을 쓸 때 대기업에서 나온 것만 쓰다 보면 효과는 좋지만 그로부터 거리를 두고 바라보기 어렵다. 얼마든지 로컬에서 작은 모델을 쓸 수도 있는데 정보나 방법을 몰라서 못 하는 경우도 많다. 그리고 기술에 대한 접근 방식의 다양성에 있어, 잘 사용하는 유창성뿐만 아니라 그것을 비판적으로 이해하고, 질문하는 관점까지를 아우르는 다양한 접근이 필요하겠다.
워크숍 총평	<AI 윤리 레터>의 기획 의도, 운영 현황, 지향점과 고민 등을 일반 청중에 소개하고 방향성을 정돈하는 계기로 삼고자 워크숍을 제안하였다. 두 패널리스트의 토론 내용이 발제에 맥락과 깊이를 더해주어, 2025 KrIGF 주제인 "우리가 가야할 길"에 기여할 수 있었다고 본다. 발제자 입장에서는 소기의 성과를 바탕으로 다양한 관점의 연결 및 가시화, 담론 불균형의 개선, 나아가 현실 개선에 기여하기 위해 꾸준한 노력과 전략적 정비가 요청된다. 제안 내용 중 '국제적 논의 및 연대'에 관한 내용은 시간 관계상 다루지 못하였으며, 이는 향후 활동 과정에서 실행에 옮기는 것을 목표로 한다.

2025 한국인터넷거버넌스포럼(KrIGF) 워크숍 세션 보고서

작성자 : 권현옥

세션명	인터넷 기업의 상생 및 ESG 방향성			
일시	2025. 7. 3. (목), 00:00~00:00		장소	세종대학교 광개토관 B1
참석자	사회	전영균(카카오)	발제	권현옥(카카오)
	패널	오경미(오픈넷)		성정모(광운대학교 국제통상학부 4학년)
		이정민(KISA)		
		전선민(KISDI)		

제안내용	디지털 기술은 사회의 혁신을 이끄는 동력이지만, 노인·장애인 등 사회적 약자와 특정 계층의 정보 접근, 경제 활동, 사회 참여 기회를 제한하며 디지털 격차를 심화시키는 이중성을 가집니다. 이는 사회 양극화를 고착화할 위험을 내포하고 있습니다. 인터넷 기업은 이러한 사회 변화에 대한 책임감을 갖고, 보유한 기술 자산과 역량을 사회적 약자의 기술 격차 해소와 미래 인재 양성을 위해 활용해야 합니다. 본 워크숍은 카카오의 ESG 실천 사례를 중심으로, 인터넷 기업이 어떻게 상생을 구현하고 지속 가능한 사회적 가치를 창출할 수 있는지 논의하고자 기획되었습니다.
요약내용	본 워크숍에서는 발표자의 모두발언을 통해 카카오의 상생 활동 사례를 중심으로 인터넷 기업의 사회적 책임과 ESG 방향성이 논의되었습니다. 디지털 격차라는 사회적 문제를 해결하기 위해 카카오가 자사의 기술과 플랫폼을 활용하여 진행하는 다양한 프로그램들이 소개되었습니다. 구체적으로 시니어 계층을 위한 '찾아가는 시니어 디지털 스쿨', 아동·청소년을 위한 '사이좋은 디지털 세상', 소상공인을 위한 '카카오클래스', 그리고 청년 인재 양성을 위한 '카카오테크 캠퍼스' 및 '카카오테크 부트캠프' 등의 사례가 제시되었습니다. 이어지는 토론에서는 해당 활동들의 사회적 가치를 재확인하고, 프로그램의 확장성과 지속가능성을 위한 제언이 오갔습니다.

논의 세부 내용	카카오의 상생 프로그램 소개와 인터넷기업의 ESG 방향성을 모색한 패널 토론으로 진행되었습니다. 먼저 발제에서는 각 계층을 위한 카카오의 맞춤형 상생 모델이 제시되었습니다. 고령층을 대상으로는 '찾아가는 시니어 디지털 스쿨'이 소개되었습니다. 이는 단순 기능 교육을 넘어, 실생활에 필수적인 디지털 활용법을 알려줌으로써 시니어 세대의 사회적 연결을 돕습니다. 특히 시니어를 '디지털 티처'로 양성해 새로운 일자리를 창출하는 선순환 구조는 기업의 사회적 책임 이행의 좋은 사례로 평가받았습니다. 아동청소년을 위해서는 '사이 좋은 디지털 세상'을 통해 사이버 폭력 예방, 디지털 윤리 등 미래 세대가 갖춰야 할 디지털 시민성을 함양하는 교육의 중요성이 강조되었습니다. 경제적 자립을 돕는 프로그램도 비중 있게 다뤄졌습니다. '카카오 클래스'는 소상공인들이 카카오 플랫폼을 활용해 스스로 경쟁력을 갖추도록 지원하며, 전국 단위의 협력 및 실질적 혜택 제공을 통해 상생의 의미를 더했습니다. 청년들을 위해서는 '카카오테크 캠퍼스'와 '카카오테크 부트캠프'를 통해 수도권과 비수도권의 교육 격차를 해소하고, 현직 개발자 멘토링 등 현장 중심의 교육으로 실무형 IT 인재를 양성하는 과정을 상세히 설명했습니다. 이어진 패널 토론에서는 발제 내용의 가치를 인정하며, 영향력 극대화를 위한 제언이 나왔습니다. 패널들은 공통적으로 카카오의 활동이 사회에 긍정적 영향을 미치고 있음을 강조하며, 이러한 우수한 프로그램들이 더 널리 알려질 수 있도록 적극적인 홍보가 필요하다는 점을 지적했습니다. 또한, 프로그램 운영을 통해 얻은 성공 노하우와 경험을 외부에 투명하게 공유하여 업계 전반으로 상생 문화를 확산시켜야 한다는 의견이 제시되었습니다. 특히 청년 패널 성정모님은 수혜자의 입장에서 구체적인 제안을 내놓았습니다. 그는 더 많은 청년이 기회를 얻을 수 있도록 프로그램의 접근성을 확대해 줄 것을 요청하는 한편, 인재 양성 프로그램의 궁극적인 목표가 기업의 인재 확보를 넘어, 교육을 통해 성장한 청년들이 다시 사회 문제 해결에 기여하는 가치 창출의 선순환 구조로 이어져야 한다고 강조해 큰 공감을 얻었습니다.

워크숍 총평	본 워크숍은 인터넷 기업이 디지털 포용성을 높이고 사회적 책임을 다하는 구체적인 방안을 카카오의 사례를 통해 성공적으로 제시했습니다. 각 세대와 계층에 맞는 맞춤형 프로그램을 통해 기술 격차를 해소하고, 미래 인재를 양성하는 활동은 기업의 ESG 가치 실현이 어떻게 구체화될 수 있는지를 명확히 보여주었습니다. 특히 패널 토론에서 제기된 홍보 강화, 노하우 공유, 접근성 확대 등의 제언은 해당 프로그램들이 한 단계 더 발전하기 위한 중요한 과제를 제시했습니다. 이러한 논의를 바탕으로 기업의 상생 활동이 사회 문제 해결의 선순환 구조로 이어질 때, 한국 인터넷 생태계 전반의 지속가능성이 더욱 강화될 것입니다.

2025 한국인터넷거버넌스포럼(KrIGF) 워크숍 세션 보고서

작성자 : 최다연

세션명	AI 기반 보이스피싱의 진화와 디지털 신뢰 체계의 위협			
일시	2025. 7. 3. (목), 00:00~00:00		장소	세종대학교 광개토관 B1
참석자	사회	김민지(숙명여대EG@IG 회원)	발제	이지현(숙명여대 EG@IG 회원)
	패널	정수민(AWS AI 보안 아키텍트 기술자)		정대규(금융보안원 침해위협분석팀 수석)
		정용욱(서울청 사이버수사과 디지털포렌식계 박사)		최다연(유로폴 사이버범죄센터 자문위원)

제안내용	현재 우리 사회는 보이스피싱 범죄의 만연으로 인해 심각한 사회적 경제적 문제에 직면하고 있습니다. 기획재정부와 경찰청에 따르면 2023년 전기통신금융사기 피해액은 약4,700억원에 달했으며 최근에도 분기별 피해 규모가 빠르게 증가하는 등 피해 확산세는 계속되고 있습니다. 전기통신금융사기의 규모는 단순 피해 건수뿐 아니라 피해 금액, 수법 정교화, 연령층 다양화 등 전방위적으로 확대되고 있으며, 그중 '보이스피싱'과 '스미싱'은 전기통신금융사기의 대표적인 수법으로 자리 잡고 있습니다. 이번 세션에서는 이 두 가지 유형을 중심으로 전기통신금융사기 발생의 사전.진행.사후 단계별 주요 쟁점과 대응 방안을 살펴볼 예정입니다. 보이스피싱과 스미싱 범죄는 심리적, 사회적, 기술적, 제도적 취약점을 종합적으로 악용하는 고도화된 디지털 범죄로 진화하고 있습니다. 단순한 전화나 문자 사기를 넘어, 최신 AI.IT 기술과 심리 조작 기법이 결합하며 탐지와 대응이 어려워지고 있습니다. AI는 단 몇 초의 음성 샘플만으로 특정인의 목소리와 억양을 정교하게 복제하고, 얼굴과 음성을 합성해 가족이나 유명인을 사칭하는 가짜 영상을 만들어 투자 유도나 신분 사칭 등에 악용됩니다. 스미싱 범죄는 '택배', '공공기관', '지인 청첩장' 등 일상적 메시지를 위장해 악성 링크를 전송하고 이를 클릭한 사용자를 가짜 사이트나 악성 앱 설치로 유도해 금융 정보와 개인정보를 탈취합니다.
요약내용	**보이스피싱과 사회적 영향** o 보이스피싱의 개념: 전화·문자·메신저 등 전기통신 수단을 이용한 금융사기 o 범죄 현황: - 연간2만~3만 건, 매일 평균22억 원 피해

- 발생 건수는 감소했으나 건당 피해액은 증가(2019년1700만 원→ 2022년2500만 원)
o AI와 결합한 신종 수법: 딥보이스·딥페이크 기술을 활용해 가족/지인 목소리·얼굴을 합성→ 신뢰 기반 붕괴
o 사회적 파급력: 개인 피해를 넘어 로이어짐

AI와 보이스피싱: 주요 개념

o 딥보이스: 억양·호흡·감정까지 재현, 실시간 합성 가능
o 발신번호 변작: 가족·지인 번호로 위장, 피해자가 속을 수밖에 없는 구조
o 딥페이크 영상: 얼굴까지 합성해 납치 협박·금전 요구
o 해외 사례: 홍콩 기업CFO 딥페이크 사기→ 350억 원 송금
o 국내 사례: 부모에게 딸 목소리로 협박 전화, 실제 목소리와 구분 어려움

심리학적 관점(최다연)

o 심리 기제 악용:
- 권위에 대한 순응(검찰·경찰 사칭 시 자동 복종)
- 긴급성 트리거(즉시 송금하지 않으면 위험)
- 정서적 신뢰(로맨스피싱: 장기간 교류 후 피해자가"속을 리 없다"는 인지부조화에 빠짐)
- 유사성 효과(딥페이크·딥보이스→ 지인·가족으로 착각)
o 2차 심리피해: 자책·낙인·불안으로 신고 주저, 사회적 고립 심화
o 국제 대응 사례:
- 영국Action Fraud : AI 분석+ 피해자 심리안정 지원, 피싱 이메일 차단율72%
- 싱가포르ScamShield : 실시간 의심 문자 경고, 블랙리스트 공유, 개인정보 보호 병행
o 한국의 현황: 통합신고센터·사후지원제도 있음, 그러나 심리적 대응은 초기 단계
o 제안:
- 실시간 심리 경고("보이스피싱 가능성 감지→ 잠시 멈춤")
- 신고-분석-차단의 구축(현재3~7일 지연 문제 극복 필요)

기술적 관점(정수민)

o AI 보이스피싱 기술:
- SV2TTS, VITS, YourTTS → 단 몇 초 샘플로도 실시간 음성 합성
- NLP 기반 스미싱→ 수천 건의 신뢰성 높은 피싱 메시지를 자동 생성
o 국내 통신사대응:

	- LGU+: 안티 딥보이스 탐지 시스템 - SKT: Scam Bank Guard (행위 기반 위협 탐지·사전 경고) - KT: 실시간 통화AI 탐지·경고(후후 앱 연동) o 한계: - 공격자는 제약 없이 신기술 활용 - 방어자는 법적·정책적 제약으로 항상 속도 뒤처짐 o 대응제안: - 합성음성 탐지·워터마크 삽입 기술 고도화 - 플랫폼·통신사 간 구축 - AI 생성물 표시 의무화 및 법적 규제 마련 - 사용자 보안 교육 및 훈련 강화 **금융권 대응(강대규)** o 금융보안원 역할: 금융권ISAC 운영, 침해사고 대응, 위협 인텔리전스 보고서 발간 o 보이스피싱 대응: - 피싱사이트·악성앱 탐지→ KISA 연계 차단 - FDS(이상금융거래 탐지) → 금융사 간 공유 - 사기 정보 공유체계 운영(금융사·수사기관·통신사·보안업체 협력) o 위협 인텔리전스 사례: - Shadow Voice (보이스피싱 조직 기법 분석) - Operation Black Echo (모듈화 공격) - Operation Midas (불법HTS 투자사기) o 신종금융사기: NFC 릴레이 결제 사기, ATM NFC 출금 피해 o 핵심 메시지: 기술·제도 협력도 중요하지만 최종 보루는 이용자의 보안의식 **수사·포렌식 관점(정용욱)** o 포렌식 경험: 25년간 디지털 포렌식→ 최근 텔레그램 투자사기 사건 다수 접수 o 사례: 신분증·회사정보 도용, 장기간 투자 유도→ 피해액 수십억~수백억 o 문제점: 피해 환수·수사 장기화(최대8년 이상 소요된 사례도 존재) o 문화적 확산: 보이스피싱 조직 실체가 영화(「시민 덕희」 등)로 재현 o 법제화 동향: - EU AI Act (위험도 기반 규제, 8대 영역 금지) - 미국AI 행동강령(2024 시행) - 한국AI 기본법(2025 제정, 2026 시행 예정) → 세부 규정은 미비 o 제안: - AI 맹신 위험 경고(부정확 정보·오류 가능성 존재)

	- 경찰청'프리캅스' 범죄위험도 분석시스템 운영(범죄 다발 지역 예측·순찰 강화) - AI 기술은 긍정적 기회와 부정적 위협을 동시에 지니므로 제도적 관리 필수
논의 세부 내용	**2) 1. AI 기반 보이스피싱의 현황과 위협** **가) 1-1. 보이스피싱의 발생 현황과 피해 규모** • (중요) 국내 보이스피싱은2006년 이후 지속 증가, 2019년 약3만7천 건으로 정점 • 최근 건수는 감소했으나 (2019년1700만 원→ 2022년2500만 원) • 단순 송금 요구에서 악성 앱, 개인정보 탈취, 대출 실행까지 로진화 • 매일 약22억 원 규모의 피해 발생, 사회적 불안 확산 **1.1-2. AI 기술 결합으로 인한 새로운 위협** • (중요) 활용→ 가족·지인 목소리 및 얼굴 합성 • 발신번호 변작과 결합 시, 실제 가족에게서 걸려온 전화로 착각→ 피해 불가피 • 2025년 사례: 딸의 목소리를 복제해 납치빙자 협박, 얼굴 합성 딥페이크 영상으로 금전 요구 • 해외 사례: 홍콩 대기업CFO 음성 합성 사기→ 350억 원 송금 피해 **2.1-3. 사회적 파급력** • 단순 금전 범죄를 넘어 문제로확장 • 목소리·사진·전화번호·메시지 등 기존의 신뢰 기반 요소가 모두 위조 가능 • 사회 전반에"누구를 믿을 것인가"라는 근본적 불안 조성 **3) 2. 심리학적 관점에서 본AI 보이스피싱(최다연)** **가) 2-1. 보이스피싱의 심리 조작 메커니즘** • (중요) 권위에 대한 순응: 검찰·경찰 사칭 시 피해자가 자동 복종 • 긴급성 트리거: "지금 송금하지 않으면 체포" → 사고 시간을 단축시키며 판단 마비 • 정서적 신뢰: 로맨스피싱→ 피해자가"속을 리 없다"는 인지부조화에 빠짐 • 유사성 효과: 딥보이스·딥페이크를 통한 지인 사칭→ 심리적 혼란 유발 **3.2-2. 피해자의 심리적2차 피해**

- 신고를 주저하게 만드는 자책감, 수치심, 낙인 우려
- 피해 이후에도 불안·우울·심리적 고립으로 장기적 상처 지속
- 따라서 단순한 경제적 구제뿐 아니라 이필수

4.2-3. 국제적 대응 사례

- 영국: Action Fraud 시스템→ AI로 유형 분석, 피해자 심리 안정 기능 포함
- 싱가포르: ScamShield 앱→ 실시간 문자·통화 분석, 위험 점수 부여, 블랙리스트 공유

5.2-4. 한국의 현황과 제언

- 2023년 통합신고센터, 사후지원 제도 마련→ 진전은 있으나
- 제안:
    - 실시간 심리 개입 기능("잠시 멈춤" 경고 인터페이스)
    - 신고-분석-차단을 연결하는 (현재3~7일 지연 문제 개선 필요)

4) 3. 기술적 관점에서 본 대응 전략(정수민)

가) 3-1. AI 기반 보이스피싱 기술

- 딥보이스: SV2TTS, VITS, YourTTS → 몇 초의 음성으로 실시간 합성 가능
- 스미싱: NLP·생성형AI 활용→ 수천 건의 신뢰성 높은 피싱 메시지 자동 작성
- 대화형 스미싱 가능→ 사용자가 답변 시, AI가 실시간으로 이어가는 공격

6.3-2. 국내 통신사 대응 사례

- LGU+: 안티 딥보이스 탐지 기술
- SKT: Scam Bank Guard → 행위 기반 위협 탐지 및 사전 경고
- KT: AI 기반 실시간 통화 분석 및 경고(후후 앱 연동 서비스)

7.3-3. 기술적 한계와 문제점

- 공격자는 법적·윤리적 제약 없이 신기술 즉시 사용
- 방어자는 법적 규제와 정확성 문제 때문에 대응 속도 느림
- 실시간 탐지에서는 속도와 정확성 사이의 균형이 어려움

8.3-4. 제안되는 대응 방향

- 합성음성 탐지·워터마크 삽입 기술 고도화
- 통신사·플랫폼 간 구축
- AI 생성물에 대한 표시 의무화 및 제도적 규제 필요
- 사용자 보안 교육·시뮬레이션 훈련 강화

5) 4. 금융권의 대응 전략(강대규)

가) 4-1. 금융보안원의 역할

- 금융권ISAC 운영: 침해사고 대응 및 정보 공유
- 위협 인텔리전스 보고서 발간: 보이스피싱 및 금융사기 분석

9.4-2. 구체적 대응 체계

- 피싱 사이트·악성 앱 탐지 후KISA 연계 차단
- 이상금융 거래(FDS) 탐지 및 금융사 간 정보 공유
- 사기 정보 공유체계 구축: 금융사·수사기관·통신사·보안업체 협력

10.4-3. 위협 인텔리전스 주요 사례

- Shadow Voice: 보이스피싱 조직 공격기법 분석
- Operation Black Echo: 모듈화된 공격 방식 등장
- Operation Midas: 불법HTS 통한 투자사기 조직 추적

11.4-4. 신종 금융사기 사례

- NFC 릴레이 부정결제
- ATM NFC 출금 사기

12.4-5. 제언

- 기관·수사기관·보안업체 간 긴밀한 협력 필요
- 법적·제도적 지원 체계 강화
- (중요) 아무리 강력한 기술적 대응이 있더라도

6) 5. 수사 및 포렌식 관점(정용욱)

가) 5-1. 포렌식 경험과 실제 사례

- 텔레그램 투자사기: 신분증·회사 정보 도용으로 신뢰 구축, 장기간 투자

	유도→ 거액 피해
	• 피해금 환수 및 수사 절차 장기화: 최대8년 이상 소요된 사례 존재
	
	13.5-2. 문화적 확산
	
	• 영화「시민 덕희」, 해외 보이스피싱 조직 영화 사례→ 실제 사건 구조와 유사
	
	14.5-3. 법·제도적 동향
	
	• EU: AI Act (위험도 기반 규제, 8대 위험 영역 금지)
	• 미국: AI 행동강령(2024 시행)
	• 한국: AI 기본법(2025 제정, 2026 시행 예정) → 세부 시행령 미비
	
	15.5-4. 제언
	
	• AI 맹신의 위험성 경고(정보 신뢰도·부정확성 문제)
	• 경찰청'프리캅스' 범죄위험도 분석시스템 운영(범죄 다발 지역 예측·순찰 강화)
	• AI 기술은 기회와 위협이 공존하므로
	
	7) 6. 종합 결론
	
	• AI 기반 보이스피싱은
	• 대응책:
	  ○ 기술적(합성음성 탐지, 워터마크 삽입)
	  ○ 제도적(법제화, 통합 대응체계)
	  ○ 심리적(실시간 경고, 피해자 회복 지원)
	  ○ 금융·수사 협력(정보 공유·초국경적 대응)
	• (중요) "사람을 바꾸는 것이 아니라, 사람이 속지 않아도 되는 구조를 설계하는 것"이AI 시대 신뢰 사회 구축의 핵심

워크숍 총평	AI 기반 보이스피싱이 가져오는 현실적 위협과 그로 인해 흔들리고 있는 디지털 신뢰 체계의 문제를 다층적 관점에서 조망했다는 점에서 의의가 크다. 단순히 기술적 문제를 논하는 데 그치지 않고, 심리학·금융·수사·국제 협력 등 다양한 분야의 논점을 아우르며 다중이해관계자적 접근의 필요성을 보여주었다는 점은 긍정적으로 평가된다. 특히 발제와 토론 과정에서 딥보이스·딥페이크 사례, 심리적 조작 메커니즘, 금융권의 위협 인텔리전스, 그리고 제도적 대응의 필요성이 구체적으로 제시되면서 청중에게 실질적인 문제의식을 환기시킨 점이 돋보였다. 학생 발표임에도 불구하고 치밀한 자료 조사와 고민의 흔적이 엿보였다는 점 또한 주목할 만하다.

	이번 세션은AI 시대에 신뢰를 어떻게 다시 설계할 것인가라는 근본적 질문을 던졌다는 점에서 의미가 크며, 앞으로 학술적 연구와 후속 논의를 통해 구체적이고 실천 가능한 대안을 발전시켜 나가기를 기대한다.

2025 한국인터넷거버넌스포럼(KrIGF) 워크숍 세션 보고서

작성자 : 희우(진보네트워크센터)

세션명	인권과 평화를 위협하는 군사 인공지능, 이대로 괜찮은가			
일시	2025. 7. 3. (목), 16:20~17:50		장소	세종대학교 광개토관 B1
참석자	사회	고아침(AI 윤리레터)	발제	자유토론방식으로 진행
	패널	박해룡 (KISA 정보보호산업본부 보안기술단 단장)		뎡야핑 (팔레스타인평화연대)
		김윤명 (디지털정책연구소 소장)		Kate Sim케이트 심 (Organizer with the No Tech for Apartheid campaign and part of the Fired Fifty for Google 416 action in 2024. Organizer with the Tech Workers Coalition)
		김한민영 (국제앰네스티 한국지부)		

제안내용

최근 팔란티어와 같은 군수기업이 국가 안보, 국방 분야에 인공지능 기술을 대거 확산시키고 있습니다. 군사 영역에 사용되는 인공지능은 단순 보조 기능을 넘어 감시와 표적 식별, 시뮬레이션 및 전투 지휘, 살상까지 인간의 생사결정에 직접 관여하는 수준으로 발전하고 있습니다.

실제로 이스라엘의 가자지구 공습 과정에서 인공지능 기반 표적 추천 시스템인 '라벤더(Lavender)'가 대량의 표적을 자동 생성해 인간의 개입 없이 살상 목표를 설정하는 데 사용되었다는 사실이 밝혀져 국제사회의 우려를 불러일으켰습니다. 기술이 인간의 생사결정에 직접 관여하는 단계로 진입한 것입니다.

한국에서도 군사 인공지능 도입이 빠르게 가속화되고 있습니다. 최근 개최된 국제 방산·안보 컨퍼런스에서는 무인기, 자율 무기 체계, AI 기반 지휘통제 시스템 등이 주요 의제로 다루어졌고, 정부와 방산업계는 AI 기술을 국방력 강화의 핵심 동력으로 삼고자 적극적으로 투자와 연구개발을 추진하고 있습니다. 국방부는 '첨단과학기술 기반 스마트 국방혁신' 전략을 통해 AI 무기체계 개발과 배치를 본격화하겠다고 밝히기도 했습니다.

그러나 이러한 기술 확산 속도에 비해 군사 인공지능이 초래할 수 있는 인권·사회적 문제에 대한 논의는 매우 미흡한 상황입니다. 민주적 통제와 투명성 확보 방안도 사실상 부재합니다.

이번 워크숍을 통해 군사 인공지능 기술의 현재와 위험성을 짚고, 인권·안보·기술적 시각에서 우리 사회가 어떻게 대응해나가야 할 지를 모색하고자 합니다. "기술은 중립적이지 않다"는 점을 분명히 하고 인간 통제 없는 전쟁이 현실이 되는 것을 막기 위한 사회적 토대를 마련하는 자리가 되고자 합니다. 나아가 무기화되는 인공지능 기술에 대한 민주적 규제, 국제 협력, 윤리적 기준 마련의 필요성을 환기하고, 이를 위한 시민사회의

	역할을 함께 논의하고자 합니다.
요약내용	제14회 한국 인터넷거버넌스포럼(KrIGF) 세션7은 군사 인공지능(AI)이 인권과 평화에 미치는 위협을 다루었다. 최근 군사 영역에 사용되는 인공지능은 단순 보조 기능을 넘어 감시와 표적 식별, 시뮬레이션 및 전투 지휘, 살상까지 인간의 생사결정에 직접 관여하는 수준으로 발전하고 있는 상황이다. 박해룡 단장(한국인터넷진흥원)은 자율 살상 드론, 무인 전차, AI 감시·분석 시스템 등 AI의 군사적 활용 사례를 소개하며 민간인 피해·통제 불가능성 등 인권 문제를 지적했다. 그는 '의미 있는 인간 통제(MHC)'와 민간지역 회피 알고리즘 같은 안전장치가 필요하다고 강조했다. 김윤명 소장(디지털정책연구소)은 자율무기의 가장 큰 문제를 '책임 공백'이라 규정했다. 개발자·지휘관·운용자 누구에게 책임을 물을 수 없는 상황이며 국가안보 명목의 규제 예외가 국제·국내 법제에서 반복되고 있다고 비판했다. 이화영 부소장(사이버안보연구소)은 AI 에이전트 개념과 '국방 메타파워' 전략을 설명하며, 이스라엘-하마스 전쟁에서 민간인 학살이 AI 의존으로 강화된 사례를 언급했다. 또한 오작동·해킹에 대비해 안전모드로 전환하는 "사이버 AI 킬스위치" 같은 안전장치가 필요하다고 제안했다. 김한민영 캠페이너(국제앰네스티)는 자율무기가 생명권·존엄권을 직접적으로 위협한다고 지적하며 대인 자율무기 전면 금지와 구속력 있는 국제조약을 촉구했다. 뎡야핑 활동가(팔레스타인평화연대)는 팔레스타인 사례를 통해 이스라엘이 팔레스타인 점령 과정에서 라벤더·합수라·아빠어디야 같은 AI 프로그램으로 민간인을 무차별 공격하고 있음을 소개했다. 또한 이를 "세계 최초의 AI 집단학살"이라고 규정하며 빅테크 기업들이 이 학살에 공모하고 있음도 밝혔다. 케이트 심 활동가(Organizer with the Tech Workers Coalition)는 구글·아마존이 이스라엘 정부와 체결한 프로젝트 님버스 계약을 비판하며 빅테크가 팔레스타인 점령과 집단학살에 직접적으로 기여하고 있다고 말했다. 아울러 노동자들의 항의가 내부 검열·집단 해고로 이어진 사실을 공유하며 국제적 연대와 저항을 호소했다. 세션 토론에서는 "유의미한 인간 통제(MHC)"의 실효성, 국제 조약의 한계, 시민사회의 대응 가능성이 주요 쟁점으로 논의되었으며 군사 AI는 단순한 안보 문제가 아니라 인권·국제법·민주주의의 근간을 위협하는 긴급 사안이라는 점이 확인되었다.
논의 세부 내용	첫 번째 토론자인 박해룡 단장(한국인터넷진흥원)은 군사 영역에서 인공지능이 실제로 어떻게 활용되고 있는지 구체적인 사례를 제시했다. 그는 자율 살상 드론, 무인 자율 전차, AI 기반 감시 및 행동 분석 시스템, 전장 예측 모델, 전쟁 시뮬레이션, 전쟁 포로 심문 AI, 병사 건강 모니터링, 부상자 후송 우선순위 결정, 통신 해독기 등 10가지 활용 사례를 나열하며 이러한 기술이 인권을 위협하는 양상을 지적했다. 특히 자율 무기 체계가 민간인과 전투원을 명확히 구분하지 못하거나 오작동 시 통제가 어렵다는 점에서

	심각한 문제가 발생할 수 있다고 보았다. 이러한 문제를 완화하기 위해서는 민간지역 회피 알고리즘의 적용, 작동 전후의 반복적 검증 절차, 데이터 수집·저장을 최소화하는 원칙, 그리고 무엇보다도 '의미 있는 인간 통제(MHC)'의 제도적 보장이 필수적이라고 강조했다. 두 번째 토론자인 김윤명 소장(디지털정책연구소)은 자율 무기의 통제와 법적 공백 문제를 심도 있게 다루었다. 그는 22세기를 '자율무기의 시대'로 규정하며 자율 무기의 가장 큰 문제는 책임 소재가 불분명하다는 점이라고 지적했다. 재래식 무기는 인간의 판단과 지휘에 의해 사용되지만 자율 무기의 경우 AI가 독자적으로 공격을 실행할 수 있어 개발자, 현장 지휘관, 운영자 중 누구에게 책임을 물을 수 있는지가 불투명하다는 것이다. 더불어 AI의 판단이 본질적으로 확률적이기 때문에 민간인 피해가 불가피하다는 점도 강조했다. 또한 현재 한국의 인공지능 기본법과 EU AI법 모두 국가안보를 이유로 군사적 AI에 대한 규제를 예외로 두고 있다는 점을 지적하며 이로 인해 규제 공백이 발생하고 있다고 설명했다. 그러면서 국제적 논의도 2014년부터 이어져 왔지만 여전히 구속력 있는 조약이 마련되지 못하고 있다는 점에서 법제도의 한계를 넘어 시민사회와 국제사회의 지속적 압력이 필요하다고 주장했다. 세 번째 토론자인 이화영 부소장(사이버안보연구소)은 'AI 에이전트'와 '국방 메타파워' 개념을 중심으로 AI의 군사적 활용을 분석했다. 그는 인공지능이 사람의 감각기관을 대체·보완하는 형태로 발전하고 있으며, 이를 종합적으로 결합한 멀티모달 AI가 전장에서 지휘관의 판단을 지원하는 방식으로 활용되고 있다고 설명했다. 실제로 팔레스타인 점령 사례에서 이스라엘 지휘관들이 AI의 분석을 합리적 근거로 수용하면서 민간인 학살이 정당화되는 사례가 나타나고 있다는 점을 경고했다. 또한 데이터셋의 품질이 충분하지 않을 경우 오류가 발생해 민간인 피해로 직결될 수 있다고 지적했다. 마지막으로 한국 국방부가 이미 '국방 메타파워'라는 개념을 도입해 AI와 사이버 전장을 결합하는 전략을 추진하고 있다고 밝히고 오작동이나 해킹 위험에 대비해 전체 시스템을 안전모드로 전환할 수 있는 '사이버 AI 킬스위치' 개념을 대안으로 제시했다. 네 번째 토론자인 김한민영 캠페이너(국제앰네스티)는 국제인권단체의 시각에서 자율무기를 비판하면서, 자율무기가 인간 개입 없이 표적을 선정하고 공격할 수 있다는 점에서 생명권, 존엄권, 사생활권, 차별금지 원칙을 위협한다고 강조했다. 특히 이러한 무기는 법적 책임의 소재를 불분명하게 만들어 국제인권법·국제인도법·국제형사법이 보호해 온 기본 원칙과 정면으로 충돌한다는 점을 지적하고 대인 자율무기의 경우 인간의 통제 여부와 무관하게 전면 금지되어야 한다는 입장을 제시했다. 또한 알고리즘이 편향된 데이터를 기반으로 인간을 식별·분류함으로써 차별을 재생산할 위험, 인간을 단순한 데이터로 환원시켜 존엄성을 훼손하는 문제, 그리고 법적 책임의 공백이 발생하는 문제를 지적하며, 자율무기 금지를 위한 구속력 있는 국제조약 제정을 촉구했다. 다섯 번째 토론자인 뎡야핑 활동가(팔레스타인평화연대)는 팔레스타인 현장의 실제 사례를 통해 군사 AI의 위험성을 지적했다. 뎡야핑 활동가에 따르면 팔레스타인 서안지구에는 1000개 이상의 검문소가 설치되어 얼굴 인식과 생체정보 수집이 광범위하게 이루어지고 있으며, 이스라엘 군이 민간 건물과 가정집을 무차별 폭격하고 있다고 한다. 그는 팔레스타인 사례에 대해 '세계 최초의 AI 집단학살'로 규정하며, 이번 집단학살의 세

	가지 특징으로 고의성, 실시간 스트리밍, 인공지능의 활용을 꼽았다. 특히 이스라엘이 사용한 라벤더(Lavender), 합수라(Habsora), 아빠어디야(Where's Daddy) 같은 AI 프로그램은 민간인을 포함한 수많은 사람을 표적화하고 학살하는 데 활용되었다고 밝혔다. 또한 구글, 마이크로소프트 등 빅테크 기업들이 상용 AI 기술을 제공하며 이 과정에 공모하고 있다는 점을 폭로했다. 명야핑 활동가는 "전 세계로 수출되는 군사된 기술의 실험 대상이자, 이스라엘이 현재 진행 중인 인공지능에 지원하는 집단학살의 생존자로서, 팔레스타인들은 무기화된 인공지능에 재앙적인 미래를 전 세계에 경고하는 탄광의 카나리아다"라는 강력한 경고를 남겼다. 마지막으로 케이트 심 활동가(Organizer with the Tech Workers Coalition)는 빅테크 기업의 책임 문제를 제기했다. 그는 구글 아동안전팀에서 근무하다가 팔레스타인 집단학살에 대한 회사의 공모를 항의한 이유로 해고된 경험을 소개하며 '노 테크 포 아파르트헤이트(NOTA)' 캠페인을 통해 구글·아마존이 이스라엘 정부와 체결한 프로젝트 님버스(12억 달러 규모의 클라우드 인프라 계약)의 철회를 요구하고 있다고 밝혔다. 그는 AI가 민간과 군사를 동시에 지원할 수 있는 이중용도 기술이라는 점에서 빅테크의 책임 회피는 설득력이 없다고 지적했다. 또한 구글이 '제노사이드'나 '아파르트헤이트'라는 단어를 사용한 직원들에게 검열·징계를 가했고 결과적으로 50명에 달하는 노동자가 해고되었는 것도 전했다. 아울러 팔레스타인에서 사용된 기술이 결국 미국 사회에도 되돌아와 감시와 억압의 도구로 사용될 것이라고 경고하며, 이를 막기 위해서는 국제적 연대와 저항이 필수적이라는 메시지로 발제를 마무리했다. 이번 세션은 군사 인공지능의 기술적 활용과 그에 따른 인권 침해 위험, 법적·제도적 공백, 현장의 참혹한 사례, 그리고 빅테크 기업의 책임 문제를 다각도로 조명했다. 패널들은 공통적으로 유의미한 인간 통제 원칙과 구속력 있는 국제 규범 마련의 필요성을 강조했고, 특히 팔레스타인 사례는 군사 AI가 인류의 존엄을 위협하는 현실적 위험임을 드러내는 대표적 사례로 제시되었다.
워크숍 총평	이 세션은 군사 인공지능이 단순한 기술 논의가 아니라 국제정치·기업 책임·인권 현실이 교차하는 복합적 문제임을 선명하게 드러냈다. 특히 팔레스타인 현장의 사례는 추상적인 위험이 아니라 이미 진행 중인 'AI 집단학살'이라는 사실을 보여주며 논의의 긴급성을 강화했다. 또한 빅테크 기업의 공모와 내부 저항 사례는 군사 AI 문제가 국가만의 문제가 아니라 노동자·시민 모두의 과제임을 확인시켰다. 참가자들의 발언을 통해 국제 규범의 미비와 법적 공백의 틈을 타 이미 군사 인공지능이 실제로 활용되고 있음을 드러내고, 인권과 민주주의를 지키기 위한 국제적 연대와 저항이 필요함을 알 수 있었다.

2025 한국인터넷거버넌스포럼(KrIGF) 워크숍 세션 보고서

작성자 : 전선민

세션명	WSIS+20와 향후 국내외 글로벌 인터넷 거버넌스 논의 대응 방향			
일시	2025. 7. 3. (목), 00:00~00:00		장소	세종대학교 광개토관 B1
참석자	사회	박민정(KISDI)	발제	전선민(KISDI)
	패널	전영균(카카오)		오병일(진보네트워크)
		송혜인(KISA)		양지수(이화사회과학원)
		정다현(이화여대)		

제안내용	o 2025년은 세계정보사회정상회의(World Summit on Information Society, WSIS)가 개최 이후 20년 간의 WSIS 결과 이행 성과에 대한 검토가 진행됨 - WSIS+20 검토는 WSIS의 성과를 평가하고, 향후 정보사회가 나아갈 방향을 제시하기 위한 이행점검 과정 o 2005년 이후의 WSIS 결과 이행을 위해 UN 기구를 포함한 다양한 기관에서진행된 노력과 진전사항에 대해 UN 과학기술위원회(CSTD)가 UN 총회에 제출하기 위한 보고서를 발간 o 2025년 12월 16~17일 미국 뉴욕 유엔 본부에서 2025 유엔총회 WSIS+20 고위급회의를 개최할 예정임 - 동 고위급 회의에서 향후 WSIS 방향에 대한 결의가 채택될 예정이며 이는 유엔 회원국 간 협상을 통해 초안이 마련될 예정임 - 상기 WSIS+20 이후에 대한 결과문서 초안 협상 과정에서 유엔 총회 의장이 다중이해관계자의 의견을 수렴할 예정이며 이러한 과정에 한국 이해관계자의 참여 필요 o WSIS+20 리뷰 과정에서의 쟁점 - WSIS는 디지털 전환, 디지털 거버넌스를 위한 주요 플랫폼으로서의 역할이 지속되어야 하는가? - WSIS 포럼과 IGF가 다중이해관계자 플랫폼 역할 지속하기 위해서는 어떠한 역할 강화와 합의를 위한 논의가 필요한가? - 유의미한 연결성 및 디지털 격차 해소를 우선순위로 설정→ 디지털 접근의 형평성 확보 노력을 어떻게 지속할 것인가? - WSIS의 강력한 모니터링 및 책무성 메커니즘 구축을 위해서 어떤 노력이 필요한가? - IGF의 지속가능한 재원 확보 방안과 포용성 강화 노력 및 리브랜딩에 대한 한국의 입장은?
요약내용	<WSIS 성과와 한계> o (성과) -2003~2005년 제네바·튀니스 회의 이후, 사람 중심·포용적·발전 지향적 정보사회라는 비전을 국제사회에 제시 -11개 액션 라인을 통해 인프라, 교육, 보안, 문화 다양성, 윤리적 원칙 등 ICT 활용의 기본 틀을 마련 -IGF(인터넷 거버넌스 포럼), WSIS 포럼과 같은 다중이해관계자 협의 플랫폼 제도화 -SDG와의 연계로 ICT가 지속가능발전목표 달성 수단으로 명확히 자리매김 o (한계) -초기 설계(2000년대 초반)의 틀에 머물러 AI, 데이터 규범, 디지털 공공재 등 새로운 의제를 충분히 반영하지 못함

	-실행력이 부족하고, 합의 중심 구조 때문에 구속력 있는 규범·결과물 부재 -디지털 격차 해소가 선언적 차원에 머물고, 재정·역량 지원 메커니즘 미흡 -개도국·시민사회 참여는 보장되었으나, 실질적 영향력과 자원 확보 한계 <주요 쟁점과 현안> o (디지털 격차) 여전히 전 세계 인구 1/3이 인터넷 미접속 상태, 단순 연결이 아닌 의미 있는 연결(Meaningful Connectivity) 개념 필요 o (재정 메커니즘) 지속가능한 ICT 기금·글로벌 펀드 필요성 대두 o (거버넌스 구조) IGF는 시민사회·신흥 의제가 살아 움직이는 장점이 있으나, 결과물 부재에 대한 지적, WSIS는 협력적 담론의 틀은 있으나, 기술 변화 반영 속도 부족하다는 지적, 다중이해관계자(MSM)" vs "정부간 협력(Multilateral)" 논쟁 지속 o (신흥 기술) AI, 데이터 거버넌스, 개인정보 보호, 사이버보안, 환경 영향 등 신흥 이슈에 대응 필요성 대두 < 한국의 과제> o (전략적 중재자 역할) 다중이해관계자 모델에서 중재자·논의 주도자로 전략적 기회 확보 가능 o (재정 기여 및 ODA 연계) 한국이 ODA·KOICA 전략을 ICT 격차 해소와 직접 연결하여 국제적 신뢰·위상 제고 o (학계, 시민사회, 청년 참여 강화) 학계는 지표·평가 프레임워크 개발로 실질 기여 필요, 시민사회는 IGF·WSIS 플랫폼에서 개인정보·AI·인권 이슈를 제기해야 함, 한국 청년의 국제사회에 더 적극적으로 참여할 수 있도록 하는 노력 필요
논의 세부 내용	<발제 : 전선민> o WSIS의 역사 및 의의 - 2003 제네바, 2005 튀니스 회의에서 제네바 원칙과 실천계획 등 채택 - 11개 액션 라인(접근성, 인프라, 보안, 교육, 윤리, 국제협력 등) 강조 o 2025년 WSIS+20 이행점검(2025년 12월 UN 고위급회의 개최 예정)을 위한 논의 과정에서의 최근 논점 - 단순 접속이 아닌 '의미 있는 연결(Meaningful Connectivity)' 필요 - AI 윤리, 데이터 책임성, 사이버보안, 디지털 격차 해소 등을 위한 노력 필요 o WSIS+20 고위급회의에서 채택할 결과문서에 대해 현재 제시된 기초문서에 포함된 내용 - WSIS 비전 재확인, SDG·GDC와 연계 - 디지털 격차, 개인정보, AI, 데이터 거버넌스, 사이버보안, 인권 등 주요 주제 제시 o 해당 WSIS+20 논의 과정에 한국의 의견을 KrIGF 명의로 제출할 필요성 강조 <패널토론> o (전영균) WSIS+20을 통해 인터넷 거버넌스 → 디지털 거버넌스로 논의가 변화되고 있는 것으로 보이며 한국은 미·중 기술 패권 경쟁 속 중재자·조정자로서 역할 가능한 시점으로 보임 - (제안사항) 하이브리드 프레임워크(정부 주도 + 다중이해관계자 결합) 추진 제안 및 IGF의 성과물 부재 문제에 대해 최소한의 결과문서나 가이드라인 작성 필요 의견 제시 o (오병일) IGF는 시민사회가 목소리를 직접 낼 수 있는 유일한 공간으로 바텀업 방식이며 새로운 이슈 제기가 가능 - 그러나 구속력 부족, 재정적 지속가능성 취약은 극복해야할 문제 - 현재 기초문서 내용 중 "Multilateral(다자주의)" 용어가 포함되면서 정부 중심주의로 흐를 가능성에 대한 우려와 "Enhanced cooperation(강화된 협력)"개념의 모호성 지적 - (제안사항) 글로벌 개인정보 규범 강화 필요, AI 활용이 기후위기를 악화시키지 않도록 데이터 투명성 확보 노력, 플랫폼 책임성 강화, AI 글로벌 규범 제정 필요

	o (송혜인) WSIS 과정에서 시작된 IGF는 다양한 이해관계자 참여의 장이라는 점이 가장 큰 장점이며 WSIS 프로세스에서 다음의 개선 노력이 필요함 - (개선필요사항) 구속력·실행력이 부족 → 결과물/실행력 강화 필요, 디지털 격차 해소를 위한 실질적 재정·역량 지원 부족하며 ICT 기금 신설, 글로벌 펀드 조성 필요, 한국은 ODA 전략과 연계해 글로벌 사우스 지원 확대를 검토해야 함. 또한 신기술 논의(예: AI)를 적극 반영해 리딩 국가의 참여 유도 필요 o (양지수) WSIS는 협력적 담론을 지향했으나 빠른 기술 변화 반영에는 한계가 있으며 AII, 데이터 규격, 디지털 공공재 등 신흥 이슈 미포함 - 기술 변화 속도를 거버넌스가 따라가지 못하면 소수 국가·기업이 규범 선점 - (제안사항) WSIS 존재 이유·설계 철학 재검토 필요, 학계는 단순 보고서 소개 수준을 넘어서 국가별 이행 검증 지표·프레임워크 설계를 제안해야 함, 디지털 격차 해소 위한 표준 마련·ODA 사업 연계 필요 o (정다현) WSIS 용어조차 청년·일반인에게 생소하며 인식·교육 부족, WSIS 포럼은 성공 사례 공유와 글로벌 네트워크 형성의 장으로 자리잡았으나 실행력과 강제력이 미흡함 - (제안사항) 한국이 브랜딩 차원에서 WSIS 포럼에 적극 참여해야 함, 청년 참여 확대 필요, 정부·기관도 청년들의 시각을 이해하는 구조 필요 <참석자 의견> o 한국 정부가 중립적이고 책임성 있는 입장을 정립해야 하며, 협력의 주체로서 시민사회·민간을 존중하는 태도 전환이 필요하다고 지적 o IGF와 WSIS+20의 지속가능성을 위해 정부의 재정적·제도적 지원 강화가 필수라고 강조
워크숍 총평	o WSIS는 지난 20년간 글로벌 디지털 협력의 기본 틀을 제공했으나, 오늘날의 급격한 기술 발전과 규범 경쟁을 충분히 반영하지 못한 구조적 한계에 직면해 있다는 지적을 받고 있음 o 앞으로의 WSIS+20 점검과정이 단순히 성과를 점검하는 차원을 넘어, 신흥 기술 규범, 디지털 격차 해소, 지속가능한 재정 메커니즘 등 현재 지적되고 있는 이슈에 대해 논의하고 이에 대한 해결방안을 모색할 수 있는 기회가 되어야 함 o 한국이 중재자·가치 기반 리더로서 다중이해관계자 모델과 정부간 협력의 균형을 설계하고, ODA·펀드를 통한 개도국 지원, 학계·청년·시민사회 참여 확대를 통해 국제 무대에서 영향력을 강화할 수 있기를 기대

2025 한국인터넷거버넌스포럼(KrIGF) 워크숍 세션 보고서

작성자 : 김기영, 도가영

<table>
<tr><td>세션명</td><td colspan="4">불안의 시대, 당신의 정보는 안녕하십니까? - SKT 유심정보 유출 사고와 존재론적 안보</td></tr>
<tr><td>일시</td><td colspan="2">2025. 7. 3. (목), 16:40~18:00</td><td>장소</td><td>세종대학교 광개토관 B1</td></tr>
<tr><td rowspan="4">참석자</td><td>사회</td><td>민병원
(이화여자대학교 교수/ 학계)</td><td>발제</td><td>김하은 (이화여자대학교/학계)
강세은 (이화여자대학교/학계)
김기영 (이화여자대학교/학계)
도가영 (이화여자대학교/학계)
임규리 (이화여자대학교/학계)</td></tr>
<tr><td rowspan="3">패널</td><td colspan="2">심동욱 단장 (KISA, 공공계)</td><td></td></tr>
<tr><td colspan="2">이진규 이사 (네이버, 산업계)</td><td></td></tr>
<tr><td colspan="2">김현이 변호사 (법무법인 세종, 법조계)</td><td></td></tr>
<tr><td>제안내용</td><td colspan="4">● 제안 취지
2025년 4월 22일, 한국의 이동통신사 SK텔레콤에서 가입자들의 유심 정보가 대거 유출되는 사고가 발생하였다. 전례를 찾기 힘든 대규모의 정보 유출은 단순한 기술적 사고를 넘어, 수많은 이용자들에게 심리적 충격과 불안감을 야기했다. 특히 SKT의 미흡한 후속 대응과, 사고와 관련된 불확실한 정보의 확산은 이용자들의 불안을 더욱 증폭시켰다.
이번 포럼에서는 이러한 이용자들의 '불안'에 주목하고자 한다. 디지털 시대를 살아가는 오늘날, 시민들의 기저에 자리잡고 있는 불안은 종종 기술적·경제적·법적 문제에 가려져 도외시되었다. 이를 회복할 새로운 관점으로 '존재론적 안보' 개념을 도입하고자 한다. 불안은 위협의 원천이 명확한 '공포'와는 구별되는 개념으로, 이용자들은 피해가 발생하지 않았음에도 '언제든 침범당할 수 있다'는 가능성 자체로부터 불안을 경험하고 있다. 이러한 불안은 단순한 정서적 반응이 아닌, 자기 정체성의 안정성에 대한 위협, 즉 존재론적 안보의 침해로 해석할 수 있다.
이번 포럼을 통해 시민들이 느끼는 불안에 주목할 필요성을 제고하고, 각국의 개인정보보호법과 디지털 권리 제도 분석을 통해 오늘날의 법적·제도적 문제 해결 방식은 이러한 불안을 충분히 고려하고 있는지 살펴보며, 정체성, 존재, 신뢰와 같은 요소들에 있어 보다 친화적인 디지털 거버넌스의 방향을 모색하고자 한다.

● 쟁점
- 개인 정보는 개인의 정체성을 형성하는 요소인가? 그렇다면 그 범위는 어디까지인가?
- 불안은 개인이 스스로 책임져야 할 문제인가? 혹은 사회적, 구조적 차원에서 관리해야 할 문제인가?
- 개인들의 불안은 현행 법과 제도에서 충분히 다루어지고 있는가?
- 존재론적 안보와 기술의 발전이라는 두 축을 고려할 때, 이러한 '불안'은 어느 정도로 반영되어야 하는가?</td></tr>
</table>

요약내용	**1. 불안의 개념과 특징** 2025년 4월 SKT에서 가입자들의 유심 정보가 대거 유출되는 사고가 있었다. 이 사고는 수많은 이용자들에게 심리적 충격과 불안감을 야기했다. 그에 더해 SKT 후속 대응은 이용자들의 불안을 더욱 증폭시켰다. 이러한 정보 유출 사고는 현재 한국 사회에서 계속 발생하고 있어 시민들의 불안은 더욱 커질 수 밖에 없는 상황이다. 불안이란 뚜렷한 실체가 부재한 상태에서 나타나는 위기적 감정으로, 두려움과는 다른 개념이다. 불안은 불확실성과 영속성이라는 특징을 가진다. 불안은 그 근원이 무엇인지 명확하지 않고, 그럴지도 모른다는 가능성에 대해 느끼는 감정이기 때문에, 막연하게 느껴지게 된다. 또한 불안은 개인 차원의 삶과 죽음이라는 시간의 흐름 속에 끊임없이 존재한다. 불안과 유사한 감정으로 공포가 있다. 그러나 공포는 불안과는 달리 그 근원에 명확한 대상인 '적'이 존재한다. 이번 SKT 유심정보 유출사고는 불안과 공포가 공존하고 있다고 볼 수 있다. 유심정보가 유출되었다는 사실 자체만으로 이용자들은 두려움을 느끼게 되는데, 이때 느끼는 것이 공포이다. 또한 한편으로는 유출된 정보가 악용되는 등의 2차 피해 가능성에 의해 이용자들은 불안이라는 감정도 느끼게 된다. 2차 피해가 발생하지 않았음에도 불확실한 가능성 때문에 두려움에 대한 두려움을 느끼게 되는 것이다. 불안의 발생은 인간의 실존과 맞닿아 있는 문제이다. 실존은 우리의 존재 그 자체로, 삶과 죽음의 문제를 의미한다. 이 실존을 지키기 위해서 개인의 정체성, '나는 누구인가'에 대한 설명이 중요한 역할을 한다. 정체성이 가진 지속성과 안정성은 예측 불가능한 삶을 살아가는 개인에게 믿음과 확신을 주기 때문이다. 그러나 정체성의 지속성과 안정성이 결여되면, 개인은 실존적인 위협을 느끼게 되고 이에 불안이 촉발된다. **2. 정체성과 존재론적 안보** 존재론적 안보는 개인이 자신의 정체성에 대해 내적 일관성을 유지하며, '나는 계속해서 나다'라는 감각을 안정적으로 갖는 상태이다. 존재론적 안보를 확보했다는 것은 개인의 정체성이 안정적으로 유지되며 실존적인 위협을 느끼지 않는다는 것이므로, 개인은 불안을 느끼지 않는다. 이러한 안보 개념은 지금까지 사회에서 강조해온 물리적 안보와는 구별된다. 물리적 안보가 무기, 전쟁, 범죄와 같은 물리적인 위협으로부터의 안전을 의미한다면, 존재론적 안보는 정체성을 위협하는 추상적인 위협으로부터의 안전을 의미한다. 불안은 영속성이라는 특성을 가지므로 완전히 해소할 수 있는 것이 아니다. 그러므로 개인은 살아가면서 온전한 존재론적 안보를 확보할 수 없다. 개인은 불안 속에서 끊임없이 자신의 존재론적 안보를 추구하며, 불안을 해소해나가는 '과정' 속에 있게 된다. 이러한 관점에서 불안은 단순한 감정이 아닌, 계속해서 통제되고 관리되어야 하는 대상이다. 불안은 개인의 문제가 아니라 사회 전체의 차원에서 주목할 필요가 있다. 특히 기술이 고도화되며 개인의 정체성은 현실 공간을 넘어 사이버 공간에서도 확립되고 있다. 현대 사회에서 사이버 공간의 정보는 개인의 정체성을 형성하는 요소이므로, SKT 유심정보 유출 사고에서 유출된 유심 정보도 정체성의 일부라 할 수 있다. 따라서 SKT 유심정보 유출 사고는 정체성의 안정성을 위협하는 사건이며, 더 나아가 이용자들의 실존적 위협이자 존재론적 안보의 위기를 보여주는 사건이다.

3. SKT 유심정보 유출 사고 분석

1) SKT 유심정보 유출 사고 대응의 문제점과 불안 증폭

2025년 4월 18일 18시 정각에 SKT 네트워크 인프라센터의 HSS에서 이상 트래픽이 탐지되었다. 이후 4월 20일 16시 40분 경 SKT는 KISA에 유출 사고 신고를 하였다. 22일 SKT는 유심 정보 유출을 공식 확인하고 대응에 착수했다.

이러한 SKT의 유심정보 유출사고 대응 과정은 이용자들의 불안을 해소하는 것이 아니라 오히려 증폭시키는 결과를 낳았다. 불안을 증폭시킨 첫 번째 문제점은 침입 탐지 후 KISA에 신고하기까지 40시간 이상 지연되었다는 점이다. 이는 법적 신고 기간인 24시간을 위반한 것으로, 의도적 은폐가 아니더라도, 조직 내 위기 대응체계가 신속하지 못하고, 수동적이었음을 보여준다. 두 번째는 통신망 핵심 인증장비인 HSS의 보안의 취약성이다. SKT는 국민의 상당수가 이용하는 통신망이라는 측면에서 SKT의 보안 수준과 대응은 국가 기반 인프라 수준의 통신 장비에서 기대되는 수준에 크게 미치지 못했다. 세 번째로 미흡한 유심 정보 유출 대응책이다. 유심 정보 유출 사고로 이용자들이 혼란스러운 사이에, SKT는 사고에 대한 통지를 유출된 정보 주체에게 정확하게 하지 않았다. 또한 유심 정보 유출로 인한 피해 방지를 위한 대책으로 마련한 유심 교체 방침은 재고 부족 등으로 인해 실효성이 저하되었다. 마지막으로 사고에 대한 정보 전달 미흡으로 인한 책임성과 투명성 부족이다. 유출에 대한 SKT CEO의 공식 사과가 있었으나, 사고원인이 무엇인지, 책임자에 대한 징계나 후속 대응에 관한 정보가 명확하게 이용자들에게 전달되지 않았다. 이러한 4가지의 문제점으로 인해 SKT에 대한 이용자들의 신뢰가 크게 감소했고, 대응과정이 진행될수록 이용자들의 불안은 더욱 증폭되었다.

2) SKT 유심정보 유출 사고 분석 : 존재론적 안보 관점으로

SKT 유심정보 유출 사고에서 이용자들은 실존적 불안을 경험하며 정체성의 혼란을 느꼈다. 이용자들은 SKT로부터 혹은 정부로부터 자신의 정보 유출 여부, 정보 보유 주체, 피해 가능성에 대한 명확한 설명을 듣지 못한 채 장기간 방치되며, 단순한 불편을 넘어 자기 존재에 대한 통제력을 상실했다. 법적 신고가 지연되며 사태를 제때 인지하지 못한 이용자들은 기업과 제도에 대한 신뢰를 잃었다. 또한 피해에 대한 명확한 안내가 부재하여 본인의 피해 여부 및 대응 방법을 알 수 없어 혼란과 불안이 심화되었고, 실망감과 배신감을 느끼게 되었다. 이러한 감정은 이용자들의 소송 및 서비스 이탈 등의 구체적인 행동 변화로 나타나기도 했다.

SKT 유심정보 유출사고는 해킹이라는 외부 침입과 내부 시스템의 구조적 허점이 동시에 작용한 복합적 사건이다. 이용자들은 외부 해킹이 발생했다는 점에서 즉각적인 위협과 두려움을 느끼는 1차 정서적 충격을 받았다. 이어 사고원인과 책임자에 대한 정보가 공개되지 않으면서 자신이 신뢰해온 국가와 기업, 제도가 '나'를 보호하지 못했다는 인식이 불안으로 이어지며 2차 정서적 충격을 받게 되었다. 결론적으로 이용자들은 단순히 기술적인 침해를 넘어, 외부 공격에 대한 충격과 내부 시스템에 대한 신뢰 상실이라는 두 차례의 충격에 노출된 것이다.

오늘날 개인의 정체성은 이름, 개인의 사진 같은 정보 외에도 USIM에 저장된 전화번호, 인증키, IMSI 등과 같은 정보 조각들로 구성된다. USIM 정보는 사이버 공간에서 '나'를 증명하는 단순한 기술적 데이터를 넘어, 사회적으로 '나'를 증명하고 일상생활 속 정체성을 구성하는 핵심 요소다. 그러나 이런 정보는 개인만이 보유하는 것이 아니라 기업 시스템에 저장된다. 그러므로 기업의 보안이 침해될 경우, 개인의 정체성을 타인이 보유할 가능성이 발생하고, 이는 단순한 불편을 넘어 존재 그 자체에 대한 충격으로

이어진다. 현대 사회에서 개인의 정체성과 직결되는 정보 조각들은 개인이 보유하는 것이 아니라 기업의 정보 인프라에 의존하게 되므로, 개인은 불완전한 자기 입증 권한을 가지게 된다. 이로 인해 지속적인 통제력의 상실을 경험하게 되며, 자신이 누구인지를 확인받지 못하는 데서 비롯되는 존재론적 불안을 촉발한다. 더 나아가 이 불안은 정체성의 혼란으로 연결되어 결과적으로 존재론적 안보의 위기로 확장된다.

존재론적 안보의 위기는 물리적 위협의 제거만으로 해결되지 않는다. 즉, 물리적 안보가 회복되었다고 해서 개인의 정체성 혼란이나 상실감이 자동으로 해소되는 것이 아니다. SKT는 사고 발생 이후 대응 과정에서 기술적·물리적 조치를 취해 보안시스템을 복구 및 강화했다. 그러나 이러한 조치는 이용자들 내면의 불안을 해소하지 못하므로 존재론적 안보의 부재는 여전히 계속되고 있다. 이용자들의 불안이 지속되고 증폭될수록, 개인의 정체성에 대한 확신이 점차 감소하게 되면서 결국 존재론적 안보 자체가 근본적으로 위협받는 상태에 놓이게 될 것이다.

SKT 유심정보 유출사고는 존재론적 안보가 디지털 인프라에 의존하는 현대인의 삶 속에서 충분히 체감가능한 현실적 위기임을 보여준다. 또한 인간의 정체성 위기를 해결하기 위한 물리적 안보 회복 그 이상의 사회적 대응과 제도적 설계의 필요성을 시사한다.

4. 정체성 관련 국내외 법제도

1) 국내 법제도

정체성과 관련하여, 국내 개인정보보호법 제 1조와 4조에서 명시하고 있는 개인정보보호법의 목적과 법이 보장하는 권리는 국내법이 표면적으로 개인의 자기결정권과 존엄성을 고려하고 있음을 보여준다. 그러나 실제 법률 과정에서는 '존엄성','자유','권리'와 같은 추상적인 요소는 잘 드러나지 않는다.

개인정보 유출 사고 발생 시 손해배상 책임 인정 여부를 판단하는 법률 과정은 존재론적 안보나 불안 등 관념적 요소보다는 실질적 피해나 범위를 확정하는 것에 초점을 둔다. 기업의 책임인정 여부를 판단하는 기준인 정보 주체 식별 가능성, 제3자 열람 가능성, 정보 확산범위 등은 대체로 물리적인 사실에 근거한다. 정보 주체의 불안감, 정체성에 대한 위협, 자기 통제권 상실을 비롯한 주관적이고 실존적인 요소들은 고려되지 않거나 증명 가능성이 낮아 법적 판단에서 실질적으로 반영되지 못하고 있다.

또한 개인 정보 유출 사실 자체만으로는 정신적 손해를 인정하기 어렵다는 대법원 판례에서 볼 수 있듯, 실질적 불이익이나 권리 침해에 대한 구체적 입증이 어려운 정서적, 실존적 피해는 법적 손해로 판단되기 어려운 것이 현실이다. 국내 개인 정보 유출 사고와 유사한 쟁점을 다루는 해외 판례를 살펴보면, 한국에 비해 미국, 일본은 불안감 자체를 손해로 인정하는 경향이 더 강하고, 피해자의 심리적 고통을 넓게 보호하려는 태도를 보이고 있다.

2) 미국 개인정보 보호법 체계

미국의 개인정보 보호법 체계는 분산형, 산업별 규제 방식으로 운영된다. 포괄적인 일반법이 존재하지 않고, 각 주 및 산업별로 개별 규제가 존재한다. 가장 대표적으로는 캘리포니아 주의 소비자 개인 정보 보호법(CCPA)가 있으며, 이 법은 점점 강화되는 추세이다. 미국은 개별적 규제 체계로 운영되면서도 미국의 법적·사회적·경제적 요인으로 인해 개인 정보 보호가 일정 수준에서 강하게 작동한다. 먼저 미국은 개인의 권리 침해에 대한 민사소송이 활발하기 때문에, 기업이 잠재적인 거액의 배상 책임과 평판 손상을 두려워하여 자발적으로 개인정보보호 정책을 엄격하게 운영하는 경향이 있다. 이외

에 강력한 산업별 규제, 주 차원의 혁신적 입법 경쟁, 시장과 소비자의 압력, 규제기관의 단속 등 다층적 억제 체계를 형성하며 기업의 '자발적 규제'를 강력히 유도한다.

3) 유럽 개인정보 보호 체계

유럽 연합은 개인정보를 단순한 '사생활 보호'가 아닌 시민의 권리이자 민주주의 조건으로 간주하며 가장 강력한 보호 체계를 발전시켜 왔다. 대표적인 제도로 GDPR(일반 개인정보보호법)이 있다. GDPR은 목적 제한성, 데이터 최소화, 동의의 명확성, 접근-수정-삭제-이식권 보장, 자동화 결정에 대한 설명 요구권이라는 5가지 핵심 원칙을 가진다. 유럽 정책의 핵심은 '개인의 데이터 통제권 보장'이다. GDPR은 동의 명확성, 자동화에 대한 거부권 등을 통해 개인의 데이터 통제권을 엄격하고 세밀하게 규제한다.

구체적으로 프랑스의 사례를 살펴보자면, 프랑스는 특히 CNIL(정보 자유위원회)라는 독립기구를 통해 GDPR을 집행하고 있다. 2019년 CNIL은 Google에 5천만 유로의 과징금을 부과했으며, 더 나아가 최근에는 AI시대 속 알고리즘 투명성과 생체정보 규율을 선도하고 있다. 2022년 프랑스 보건청에서 발생한 의료정보 유출 사건 이후, 프랑스는 데이터 알고리즘 투명성 법안을 제정했고, 시민이 자동화 결정구조에 대해 설명받을 권리를 명시했다. 또한 학교와 지역단체의 개인정보 권리교육 의무화, 시민 참여 패널을 통한 공공정책 수립 등 시민의 개인정보보호에 대한 인식 제고를 위해 노력하고 있다.

4) 시사점

국내 개인 정보 보호법은 유럽과 유사한 체계를 가지고 있음에도 불구하고 개인 정보 통제권 실현이 빈약하다. 그러므로 한국 역시 존재론적 안보와 정체성 보호 시스템을 기반으로 법을 강화하는 방식의 전략 구축 필요성이 제기된다. 먼저, 개인 정보 유출로 인한 피해자의 심리적 고통을 반영하기 위해 정신적 손해 인정의 판결 기준을 확장하고, 명확하게 다듬을 필요가 있다. 또한 정보의 주인으로서 개인의 인식 변화와 개인정보 중요성을 인지하는 사회적 환경 조성이 필요하다.

5. 결론 : 존재론적 안보를 보장하기 위한 통합적 접근의 필요성

SKT 유심정보 유출 사고는 불확실성과 정체성 불안이 촉발한 존재론적 안보의 위기를 보여주는 사례다. 이 사고의 대응에서 볼 수 있듯, 현재 이러한 유출에 대한 정부와 기업의 대응은 보안 강화, 기술 업그레이드 등 물리적인 복원에 집중되고, 피해자들의 실존적 불안과 정체성 손상에 대한 고려는 미흡하다.

이러한 존재론적 안보의 위기를 해결하기 위해서는 개인과 기업, 국가 차원의 통합적 접근이 필요하다. 개인은 자신의 정보의 수집·처리·유통 관련 실질적인 통제 권한이 없고, 정체성 위기와 불안을 관리할 사회적·정서적 준비도 미흡하다. 게다가 반복된 개인정보 유출 사고로 인해 정보 유출에 대한 개인의 민감성도 낮아졌다. 정보 침해의 심각성 인지는 대응의 기본 단계이다. 따라서 개인 정보에 대한 시민의식 강화를 위한 교육과정의 설계 및 캠페인과 공공 커뮤니케이션 장 마련을 통해 개인정보의 중요성을 인지하는 사회문화 조성이 필요하다.

이와 함께 주관적이고 실존적 차원의 피해를 반영할 수 있도록 존재론적 안보의 관점에서 개인을 보호할 수 있는 방향의 법제도 개선이 이루어져야 한다. 또한 정체성 회복을 위한 실질적 권리를 법제화하려는 노력에 더해 정보 주체 중심의 회복 절차의 제도화가 이루어진다면 물리적 대응으로는 해결되지 못하는 정체성의 복원을 이룰 수 있을 것이다.

	더 나아가 초국가적 차원의 노력도 필요하다. 오늘날 정보는 인터넷을 통해 초국가적으로 유통되기 때문에, 한 국가의 노력만으로는 존재론적 안보의 위기를 해결할 수 없다. 그러므로 국가 차원의 개인 정보 보호 관련 다자/양자 협약 체결 및 강화, 국제기구 역할 확대, 글로벌 빅테크 기업에 대한 감시 메커니즘 국가 등의 초국가적 협력이 필수적이다.
논의 세부 내용	**● 패널 토론** **이진규 이사 (산업계) :** 현재 한국은 과징금을 부당이익 환수의 개념으로 접근하여, 과징금 또한 존재론적 불안을 해소하는 데 사용하고 있지 못하고 있다고 여겨진다. 이러한 환수된 부당이익으로 정부가 불안 해소를 위한 기금 조성을 하는 등의 대응 방안을 고민해볼 수 있을 것 같다. 기타 국가별로 법제도를 분석해주셨는데, 디테일하게 살펴보면 미국과 일본의 경우, 실제 배상금이 매우 작아서 실질적으로 정보주체의 권익을 보장하고 불안을 해소할 수 있는 수준으로 보기 어렵다. 그러므로 이 문제는 우리나라에 한정된 이슈가 아니라 전 세계적으로 개선되어야 할 지점이 많다는 생각이 들었다. 발제에서 우리나라의 개인정보 관련 정보 주체의 통제권이 작은 상황이라고 해주셨는데, 실제로는 우리나라의 정보 주체가 가지고 있는 개인정보 통제권은 굉장히 다양하고, 어떤 경우는 유럽보다도 더 강력하게 규제되는 부분도 있다. 하지만 아직 사회적인 분위기에서 충분하게 그와 같은 권리 보장의 분위기가 마련되지 않았으므로, 이러한 법제도와 사회 분위기의 간극을 어떻게 줄일 수 있는지의 측면에서 접근이 필요하다. 개인정보 유출로 발생할 수 있는 불안감에 대해서는 UX적인 접근을 해야 된다는 생각이 든다. 대응할 때 불안감 자체, 불안감의 증폭 요소 등을 정보 주체와의 상호작용을 통해 제대로 분석하고 프로세스 과정에서 하나씩 대응을 해나가는 절차를 마련해나간다고 하면 개인, 기업, 국가의 총체적인 측면에서 접근을 보다 강화할 수 있을 것이다. **김현이 변호사 (법조계):** 법의 가장 큰 기능과 역할 상 다양한 이해 관계자들 사이에서 피해가 발생하는 경우, 양쪽 모두에게 일정한 권리를 보호해줘야 한다. 따라서 정보 유출 피해가 발생한 경우, 피해자들에게 손해가 마땅히 보장되어야 하지만, 보호해야 할 피해 범위에 대한 별도의 논의는 필요하다. 또한 발제에서 말씀해주신 종합적인 요소를 고려하는 이유가 있다고 보는데, 확인되지 않은 사항에 대해서 다 배상하라고 인정하는 것은 다양한 사회 구성원의 합의가 이루어지기 어렵다고 볼 여지가 있다. 정신적인 피해는 개인에 따라 느끼는 정도가 다를 수 있다는 점에서 법원이 사회 일반인을 기준으로 어느 정도 확인 가능한 결과를 요구할 수 밖에 없는 측면도 고려해야 한다. 판단 기준은 결국 사회적 합의 결과이므로 항상 변화할 수 있는 부분이라 생각하며, 합의 도출까지 오래 걸리더라도 논의는 계속 진행되어야 할 분야라고 본다. 사회적 합의로 기업들의 자정 능력과 소비자들의 이해 증진의 측면에서 사회 구성원 각각 조금씩 노력함으로써 현실적 대안을 마련할 수 있을 것이라 본다. 법 제도를 통해서 해결하기 보다는 사회구성원 간 좋은 선의 합의가 이루어진다면 문제를 모두 만족할 수 있는 방향으로 해결할 수 있을 것 같다. **심동욱 단장 (공공계):** 법에서 불안을 직접적으로 명시하지 않는데, 그와 유사한 표현이라면 '우려'가 있을 것 같다. '우려'가 주로 공통적으로 등장하는 의미가 침해에 대한 우려, 걱정, 불안으로 해

	석되므로, 법 상에서는 이미 정보 주체의 불안을 어느 정도 포섭하고 있다고 생각한다. 그리고 정보 주체가 개인정보 처리와 관련된 불안감을 해소할 수 있는 장치가 법적으로 곳곳에 존재하긴 한다. 그러나 이러한 법의 내용과 장치들이 국민의 불안감을 해소하는데 충분한가에 대해서는 논의가 필요하다고 본다. 그러한 논의를 통해서 우리나라에서 지금 규율하고 있는 개인정보에 대해 사회적 합의가 이루어지면서 발전해나가고 있는 것이 아닌가 생각한다. 예방 및 대응 관련하여 우선 불안이라는 것들에 대한 정확한 소통이 중요하다고 본다. 정확한 소통과 충분한 설명이 개인정보 전 영역에서 이루어진다면 불필요한 불안을 사전·사후에 해소할 수 있을 것이다. **● 플로어 의견** **참여자 (1):** 소비자 불안 측면 관련하여, 소비자한테 리턴을 할 수 있는 방식으로서 요금 감면이 대안이 될 수 있을 것 같다. **참여자 (2):** 법은 단순한 공포나 불안에 대해서는 보상을 하지 않는다. 이러한 것에 대해서는 사회가 그것을 어떻게 해결할 것인지에 대해 초점을 두어야 한다. SK 사건 같은 경우에도 징벌이나 손해배상보다는 좀 더 예방적·사회 안정적 차원에서 해결할 방법을 생각할 필요가 있다. 실질적으로 제도를 살펴보면 다른 나라는 가지고 있지 않은 제도를 한국이 많이 가지고 있고, 더 법 제도가 강한 측면이 있다. 한국과는 달리 다른 나라는 해킹 사건을 숙명적으로 받아들인다. 그래서 다른 나라들의 최근에 나온 법들에서는 침해 예방을 하지만 신속한 복구에 초점을 두고 있다. 한국은 해킹 사건이나 개인정보 사건 발생 시, 이 문제가 도덕적 문제로 전환되어 다른 나라에 없는 제도를 계속 생산해내는 것이다.
워크숍 총평	이번 논의는 SKT 유심정보 유출 사고를 출발점으로, 개인정보 유출을 단순한 기술·보안 문제가 아닌 '존재론적 안보' 위기로 확장해 해석함으로써 새로운 시각을 제시했다는 점에서 긍정적으로 평가한다. 피해자의 실존적 불안과 정체성 손상을 물리적 복원 조치만으로는 해소할 수 없음을 지적하고, 개인·기업·국가 차원의 통합적 대응, 시민의식 제고, 법·제도의 보완, 초국가적 협력 필요성 등을 다층적으로 제안한 점이 인상적이다. 또한 패널들의 토론을 통해 존재론적 안보 개념을 손해배상과 연결하여 법제도 분석을 시도한 점, 과징금의 활용 방향 전환, UX 기반 불안 해소 절차 설계, 사회적 합의의 중요성 등 구체적이고 실천적인 논의가 이루어졌다. 다만, 해외 법제도와 국내 법제도의 비교에서 보다 세부적이고 균형 잡힌 분석이 추가된다면 논의의 깊이와 설득력이 강화될 것이다. 이는 추후 학생들의 추가 연구로 보완될 수 있을 것이라 기대한다.